UNIVERSIDADE NOVA DE LISBOA

Faculdade de Ciências e Tecnologia

Departamento de Engenharia Electrotécnica

Monitorização automática de redes de computadores

Estudo e proposta de uma nova solução

Por:

João Miguel Baia Simões

Dissertação apresentada na Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa para obtenção do grau de Mestre em Engenharia Electrotécnica e de Computadores

Orientador: Professor José Manuel da Fonseca

Lisboa

2010

Sumário

Esta tese apresenta um estudo das várias ferramentas open-source de monitorização de redes existentes no mercado, fazendo referência a algumas aplicações populares tais como o Nagios e o Zenoss. Depois de justificada a escolha da utilização da ferramenta de monitorização de redes Nagios como motor de monitorização para o desenvolvimento prático, são discutidas e analisadas ao detalhe algumas das soluções *frontend Web-based* disponíveis no mercado, apresentando-se também uma solução original de seu nome Athena.

Por fim, são comparadas as diferentes soluções apresentadas, em termos de vantagens e desvantagens e apresentados os resultados da solução Athena. Estas comparações são realizadas levando em conta a complexidade, a utilidade e a funcionalidade das diversas ferramentas.

Abstract

This master thesis presents a study of the various open-source monitor network tools that exist actually, referencing some popular applications like Nagios and Zenoss. After justifying the choice of the network monitoring tool Nagios to use as a monitoring engine in the development phase, some frontend Web-based solutions available in the market are discussed and analyzed, and an original solution named Athena is presented.

Finally the solutions presented are compared from the point of view of the advantages and disadvantages in terms of complexity, functionality and utility, and the results of the Athena solution are presented.

Índice de matérias

Sumário…… 1
Abstract…… 2
Índice de matérias…… 3
Índice de figuras…… 7
Índice de tabelas…… 9
Capítulo 1. Introdução…… 10
1.1 Motivação…… 10
1.2 A importância da monitorização de redes…… 10
1.2.1 FCAPS – Um modelo de gestão de redes…… 11
1.2.1.1. Categoria de gestão de falhas…… 12
1.2.1.2. Categoria de configuração…… 12
1.2.1.3. Categoria de contabilidade…… 13
1.2.1.4. Categoria de gestão de desempenho…… 13
1.2.1.5. Categoria de gestão de segurança…… 13
1.3. Ferramentas de monitorização…… 14
1.3.1. Monitorização com ou sem agentes…… 14
1.3.2. Principais funcionalidades…… 14
1.3.3. Tipos de ferramentas de monitorização…… 15
1.4. Sistemas de apoio à decisão…… 16
1.4.1. Tipos de sistemas…… 16
1.4.2. Implementação e características…… 16
1.4.3. Sistema de apoio à gestão…… 17
1.5. Objectivos do trabalho desenvolvido…… 17

Capítulo 2. Estado da arte…… 19
2.1. Nagios…… 20
2.1.1. Visão global…… 20
2.1.2. Requisitos e instalação…… 20
2.1.3. Arquitectura…… 22
2.1.4. Configuração inicial…… 22
2.1.5. Funcionamento…… 23
2.1.5.1. Verificações…… 23
2.1.5.2. Plug-ins…… 24

2.1.5.3. Interface Web……..... 25
2.1.5.4. Modelos……. 26
2.1.6. Resolução de problemas……... 26
2.1.6.1. Notificações…….. 26
2.1.6.2. Event Handlers……..... 27
2.1.7. Análise de resultados……..... 27
2.2. Cacti…….. 28
2.2.1. Visão global…….. 28
2.2.2. Requisitos e instalação…….. 29
2.2.3. Arquitectura…….. 30
2.2.4. Configuração inicial…….. 31
2.2.5. Funcionamento……. 31
2.2.5.1. Organização de gráficos…… 31
2.2.5.2. Criação de gráficos……... 32
2.2.5.3. Modelos…… 32
2.2.5.4. Importar e exportar modelos…… 34
2.2.5.5. Gestão de utilizadores……..... 34
2.2.6. Análise dos resultados…….. 35
2.3. Zenoss……..... 36
2.3.1. Visão global……. 36
2.3.2. Requisitos e instalação……. 36
2.3.3. Arquitectura……. 37
2.3.3.1. Camada de recolha…….. 37
2.3.3.2. Camada de processos…….. 37
2.3.3.3. Camada de dados……. 38
2.3.3.4. Camada de utilizadores…… 38
2.3.4. Configuração inicial……. 38
2.3.5. Funcionamento……. 38
2.3.5.1. Modelação de dispositivos……... 39
2.3.5.2. Interface Web…….. 39
2.3.5.3. Gestão de dispositivos……. 40
2.3.5.4. Gestão de eventos…… 41
2.3.5.5. Gráficos de desempenho……. 41
2.3.5.6. Relatórios…… 42
2.3.5.7. Gestão de utilizadores……. 44

2.3.5.8. Janelas de manutenção…… 44
2.3.5.9. ZenPacks……. 44
2.3.6. Resolução de problemas…… 44
2.3.7. Análise dos resultados…… 45
2.4. Comparação dos resultados das ferramentas……..... 46
2.4.1. Instalação e configuração…….. 46
2.4.2. Arquitecturas……..... 47
2.4.3. Apresentação e utilização…….. 48
2.4.4. Funcionalidades……..... 48
2.4.4.1. Visualização da informação e representação gráfica……..... 49
2.4.4.2. Utilização de modelos…… 49
2.4.4.3. Resolução de problemas…… 50
2.4.5. Extensões e comunidades…….. 50
2.4.6. Resultados……..... 51
2.5. O Nagios como motor de monitorização…….. 51
2.5.1. Nconf…… 51
2.5.1.1. Visão global…….. 51
2.5.1.2. Funcionalidades…… 52
2.5.1.3. Análise de resultados…… 55
2.5.2. Centreon…… 56
2.5.2.1. Visão global……..... 56
2.5.2.2. Funcionalidades…… 58
2.5.2.3. Análise de resultados…… 59
2.5.3. Opsview……... 60
2.5.3.1. Visão global……..... 60
2.5.3.2. Funcionalidades……... 61
2.5.3.3. Análise de resultados…… 62
2.6. Outras ferramentas…… 63
Capítulo 3. Descrição do trabalho desenvolvido……. 65
3.1. Configuração de rede…….. 66
3.1.1. Inserção de um novo dispositivo…… 66
3.1.2. Alteração de serviço existente…… 68
3.1.3. Adição de novo serviço……. 68
3.1.4. Criação de um horário……... 69
3.2. Informação da rede……..... 69

3.2.1. Visualização da rede……..... 70
3.2.2. Visualização de recursos……... 70
3.2.3. Visualização de horários……... 72
3.2.4. Mapa da rede……. 72
3.2.5. Visualização do estado geral da rede……..... 73
3.3. Análise da rede…….. 74
3.3.1. Relatórios……... 74
3.3.2. Comparação de recursos de rede…… 75
3.3.3. Visualização de problemas……..... 76
3.3.4. Sistema de apoio à gestão…….. 77
3.3.4.1. Análise de custos…… 77
3.3.4.2. Análise de desempenho…….. 80
3.3.4.3. Ferramenta de comparação de dispositivos…… 82
3.3.4.4. Agenda…… 83
3.3.4.5. Classificação de estados……. 84

Capítulo 4. Apresentação e comparação de resultados…….. 85
4.1. Arquitectura……..... 85
4.2. Configuração…….. 85
4.3. Apresentação…….. 86
4.4. Visualização……... 86
4.5. Análise do comportamento da rede……..... 88

Capítulo 5. Conclusões e trabalho futuro……... 91

Anexo A. Ficheiros de configuração do Nagios……. 94
Anexo B. Base de dados da solução Athena……... 98
Anexo C. Classificador baseado em árvores de decisão……..... 99
Anexo D. Tutorial de instalação do NSClient++…… 103
Agradecimentos…….. 104
Referências bibliográficas…….. 105

Índice de figuras

1.1.Estrutura do modelo TMN e relação com a gestão de redes FCAPS……. 11
2.1. Exemplo de monitorização com o NSClient++ num ambiente Windows……..... 21
2.2. Exemplo de monitorização com o NRPE num ambiente Unix……. 21
2.3. Arquitectura do Nagios……. 22
2.4. Arquitectura do Cacti…… 30
2.5. Arquitectura do Zenoss……..... 37
2.6. Comparação de ferramentas……..... 46
2.7. Arquitectura da monitorização distribuída suportada pelo Nconf…… 52
2.8. Aspecto da interface Web do Nconf……. 55
2.9. Arquitectura do Centreon…….. 57
2.10. Aspecto da interface Web do Centreon……. 58
2.11. Diagrama da arquitectura principal do Opsview……. 60
2.12. Diagrama da arquictura distribuída do Opsview……. 61
2.13. Exemplo gráfico de desempenho da carga do CPU do computador……... 62
3.1. Aspecto da interface Web do Athena…… 65
3.2. Definição de um novo dispositivo…… 67
3.3. Associação de serviços a um novo dispositivo……. 67
3.4. Alteração dos serviços a verificar num dispositivo…….. 68
3.5. Associação de uma nova verificação de um recurso a um dispositivo já existente..... 68
3.6. Criação de um novo modelo de horários…….. 69
3.7. Secção de visualização da informação da rede…… 70
3.8. Secção de visualização da informação de serviços I…… 71
3.9. Secção de visualização da informação de serviços II…….. 71
3.10. Tipos de gráficos de serviços……. 72
3.11. Alocação de um dispositivo numa sala…….. 73
3.12. Secção de mapa da rede……. 73
3.13. Secção de estado geral da rede……... 74
3.14. Exemplo de gráfico de disponibilidade de um dispositivo……. 75
3.15. Exemplo de gráfico de estado de um serviço de uma máquina…….. 75
3.16. Exemplo de comparação instantânea dos principais recursos da rede…… 76
3.17. Barra informativa do estado da rede……... 76
3.18. Secção de problemas na rede……. 77

3.19. Exemplo de análise de custo global…… 78
3.20. Exemplo de análise de custo individual I…… 79
3.21. Exemplo de análise de custo individual II…….. 79
3.22. Exemplo de utilização normal da carga do CPU……. 80
3.23. Exemplo de utilização da memória física……... 81
3.24. Exemplo de uma análise de desempenho global……. 81
3.25. Exemplo de comparação por valores médios na FCD…… 82
3.26. Exemplo de um mês na agenda……... 83
3.27. Exemplo do detalhe de uma entrada da agenda…….. 84
B.1. Modelo Entidade-Relação da base de dados do Athena…….. 98
C.1. Exemplo de classificador baseado numa árvore de decisão……. 99

Índice de tabelas

A.1. Directivas utilizadas na definição de um novo dispositivo…… 94
A.2. Directivas utilizadas na definição de um novo serviço…….. 95
A.3. Directivas utilizadas na definição de um novo período de tempo……. 96
A.4. Directivas utilizadas na definição de um novo contacto……... 96
A.5. Directivas utilizadas na definição de um novo modelo……. 97

Capítulo 1

Introdução

1.1 Motivação

O sucesso de uma empresa está dependente de inúmeros factores, como por exemplo o desempenho individual dos seus colaboradores, a manutenção do nível geral de produtividade e a utilização racional dos seus meios. Este último factor representa um dos maiores motivos de preocupação por parte das empresas, que começam a perceber que a realização de uma melhor gestão dos seus recursos pode desempenhar um papel importante na economia das mesmas. Estes meios tanto podem ser o material de escritório e os dispositivos de rede comprados e em utilização, como a electricidade consumida por estes na empresa.

Hoje em dia qualquer negócio está dependente da qualidade dos serviços de rede que só é assegurada pela garantia de um correcto funcionamento da mesma onde se encontram. Para que uma rede funcione sem problemas, é aconselhável ter alguma forma de monitorizar o seu comportamento e desempenho, e agir proactivamente para evitar o aparecimento de problemas que comprometam o seu bem-estar futuro. Todo este processo é facilitado pelas ferramentas de monitorização de redes disponíveis no mercado. Por estas razões a motivação para o desenvolvimento deste trabalho tem então por base o interesse do autor na área da monitorização de redes, tendo como objectivo perceber as vantagens resultantes da escolha da utilização de uma ferramenta deste tipo, por parte de empresas com negócios dependentes da sua rede, e ainda o interesse em estudar sistemas de apoio à decisão, analisando a viabilidade da implementação de um sistema de apoio à decisão orientada à gestão de uma rede de dispositivos e os potenciais benefícios que poderão daí advir.

1.2 A importância da monitorização de redes

Uma rede informática é em muitos aspectos semelhante a um complexo organismo vivo. Tal como este, uma rede é composta por diferentes sistemas que devem funcionar em conjunto e sem problemas de forma a garantir o bem-estar geral da mesma. Afinal, hoje em dia, a rede é quase sempre o órgão vital de uma empresa [1].

Actualmente quase todos os dispositivos informáticos presentes numa empresa estão de alguma forma ligados à rede. Muitas tarefas que no passado eram realizadas por uma pessoa sozinha no seu computador, são agora realizadas em cooperação com outras pessoas, através da rede informática. Estes são apenas alguns exemplos da enorme dependência que os negócios das empresas têm hoje das redes informáticas. O facto é que este tipo de redes têm o potencial de permitir um aumento da produtividade numa empresa, no entanto, para aproveitar estas vantagens, é necessário garantir a melhor gestão possível dessas mesmas redes.

Se a gestão realizada for deficiente, poderá ter grande impacto negativo no desempenho da empresa, poderá representar um aumento dos custos ou mesmo um prejuízo significativo. Como tal, é importante o investimento na área da monitorização de redes, como forma de garantir que tudo é bem gerido e que estão criadas e se mantêm as condições para que a empresa possa evoluir. É fácil perceber a importância da monitorização da rede de uma empresa, tanto no plano económico a nível da redução de custos associados à própria gestão da rede e dos recursos utilizados, como no plano produtivo, com consequência no desempenho da empresa no mercado, criando vantagens na sua competitividade. Por estas razões, a utilização de uma solução de monitorização de redes, em substituição da gestão realizada com base no levantamento manual das características e estados dos dispositivos da rede de uma empresa, oferece uma maior fiabilidade dos dados apresentados, uma apresentação quase instantânea do estado da rede e a possibilidade de definir alarmes automáticos para prevenção ou correcção de potenciais problemas, entre outras vantagens.

1.2.1. FCAPS – Um modelo de gestão de redes

A gestão de uma rede deve ter por base um dos vários modelos de referência de gestão de rede disponíveis. Um dos modelos mais conhecido é o FCAPS, uma extensão do modelo conceptual de gestão de redes conhecido por *Telecommunication Management Network* (TMN), que descreve a gestão de redes em quatro camadas. Cada camada do TMN executa algumas ou todas as funções do FCAPS [10]. Embora na sua maioria estes modelos sejam algo complexos para servirem de guia, são uma boa opção para definir as ideias gerais de uma gestão de redes eficiente.

O modelo FCAPS está dividido em cinco categorias que lhe dão o nome:

- Fault;
- Configuration;
- Accounting;
- Performance; e
- Security.

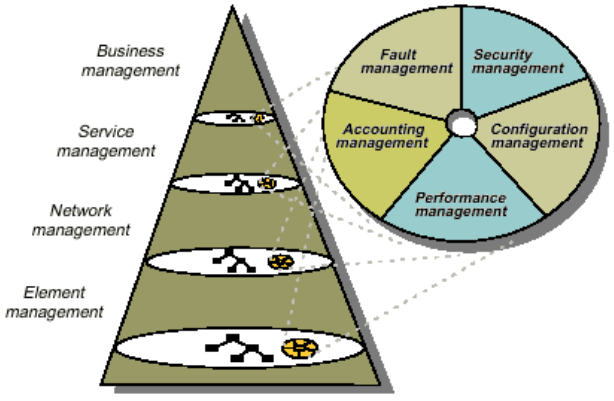

Fig 1.1 – Estrutura do modelo TMN e relação com a gestão de redes FCAPS

1.2.1.1. Categoria de gestão de falhas

A categoria de gestão de falhas tem como objectivo primordial manter uma rede funcional e sem falhas, estando dividida em três fases: a monitorização, o diagnóstico e o envio de notificações ou a correcção das falhas de uma forma proactiva. Esta última fase é das mais importantes nesta categoria, já que é com as notificações ou correcções que se podem prever ou resolver os problemas na rede, evitando que aumentem progressivamente e que criem ainda maiores problemas. Segundo esta categoria deverá existir também um meio de ver a informação relativa a todas as notificações ou alarmes enviados, listados por exemplo a partir de representações gráficas dos estados componentes da rede, devendo privilegiar-se as representações em mapas que tornem a informação mais fácil de entender. Sugere-se ainda a criação de um histórico dos alarmes dados, como forma de poder prever futuras falhas na rede. Todos os alarmes devem ser limpos do sistema, assim que os problemas que os originaram estiverem resolvidos, de forma a manter a informação do estado da rede o mais fiável ou mais perto possível da realidade.

A nível do diagnóstico das falhas é igualmente aconselhado que o sistema consiga identificar rapidamente qual a causa das falhas na rede, de forma a evitar um grande impacto nesta, já que uma notificação geralmente alerta apenas para um sintoma. Estes diagnósticos podem ser realizados se, por exemplo, se devolver mais informação sobre o dispositivo ou se se executarem outros tipos de testes remotamente. Este último processo facilita também uma actuação proactiva, ou seja possibilita detectar tendências para falhas e impedir que estas cheguem a acontecer.

Caso a rede onde se quer implementar a monitorização tenha um número muito elevado de utilizadores, poderá ser preferível implementar um sistema de fila de espera para o envio das notificações ou resolução dos ditos problemas.

1.2.1.2. Categoria de configuração

Para uma rede poder funcionar e ser monitorizada, é necessário que seja devidamente configurada. Esta configuração consiste em descobrir a rede, os dispositivos que lhe pertencem e que se querem monitorizar, bem como os recursos e serviços.

Para que não seja necessário estar constantemente a verificar a rede para saber a sua configuração, esta categoria sugere que haja uma sincronização entre o sistema de monitorização e a rede propriamente dita. Esta sincronização pode ser feita guardando a informação que não costuma variar muito (estática) da rede, numa base de dados. Como este tipo de informação não é informação estatística, como o é por exemplo o desempenho dos componentes da rede ao longo do tempo, é possível manter a informação quase sempre actualizada.

Um sistema de gestão deve ainda proteger o sistema, garantindo a existência de cópias do mesmo, de forma a ser possível restaurá-lo em caso de algum problema mais grave, como a infecção por um vírus, por exemplo.

1.2.1.3. Categoria de contabilidade

A gestão da contabilidade numa rede é também importante se a empresa oferecer algum serviço através desta. Esta é a forma que as empresas têm de garantir lucro a partir dos serviços que disponibilizam. A gestão de contabilidade suporta ainda auditorias e comunicação de fraudes, analisando comportamentos suspeitos ou pouco comuns [9].

1.2.1.4. Categoria de gestão de desempenho

A gestão de desempenho implica que se monitorize a rede e se faça alterações para garantir que o seu desempenho não influencie negativamente a qualidade de serviço que foi acordada com os seus utilizadores, nos *Service Level Agreements* (SLA). É aconselhada uma análise a vários parâmetros na gestão da rede, como por exemplo os atrasos na realização de determinadas tarefas, como o envio de notificações. Esta gestão de desempenho poderá ser facilitada com o recurso ao uso de gráficos que apresentem as tendências desses parâmetros, sendo por vezes possível identificar padrões de comportamento que permitem antever a ocorrência de um problema.

1.2.1.5. Categoria de gestão da segurança

A última categoria diz respeito à gestão da segurança numa rede. Os aspectos da segurança podem ser divididos em dois grupos bem distintos: a gestão da segurança e a segurança da gestão.

A segurança da gestão tem a ver com as operações de gestão, se são seguras e realizadas apenas por utilizadores autorizados. É necessário garantir, por exemplo, que não há alterações de configuração de dispositivos por parte de um utilizador que não tem o nível de autorização necessário para o fazer. Estas medidas podem ser garantidas com variadas acções, como por exemplo definir privilégios e listas de acesso e requisitar palavras-chave difíceis de decifrar ou obrigar à sua alteração periódica.

Por sua vez, a gestão da segurança é relativa à segurança da rede, ou seja em vez de evitar que o sistema esteja vulnerável às pessoas que o utilizam (quem está por dentro), evita-se que esteja vulnerável ao exterior, como por exemplo a ataques de intrusos ou *hackers*. Alguns exemplos de acções que podem ser tomadas para evitar falhas de segurança deste tipo são a criação de uma lista negra de acessos, onde se bloqueiam portos e endereços de IP que apresentem padrões de tráfego suspeitos, ou a monitorização dos pacotes que são trocados na rede para detectar qualquer anomalia.

1.3 Ferramentas de monitorização

A utilização de uma ferramenta de monitorização dos dispositivos, recursos e serviços de uma rede possibilita melhorar muitos aspectos de uma organização. O conceito base do funcionamento de uma ferramenta de monitorização é a execução de verificações periódicas, a recepção dos resultados vindos dos diversos dispositivos com os quais está a comunicar e o tratamento desses dados para apresentação ao gestor da rede. A ferramenta disponibiliza, normalmente através de uma interface, a informação recolhida num formato *user-friendly* que tem como objectivo facilitar a interacção do utilizador com o sistema.

1.3.1. Monitorização com ou sem agentes

Para se poder monitorizar dispositivos, é necessário escolher um método de recolha da informação remota. Existem duas formas de o fazer, recorrendo à utilização de aplicações agentes ou sem as utilizar. A monitorização sem agentes é normalmente realizada com recurso a um protocolo de comunicação como o SNMP, ou o SSH. Embora seja mais rápida, dado que não tem como requisito a instalação de agentes nas máquinas remotas, não permite grande detalhe nas verificações, consistindo assim, na maior parte das vezes, apenas na informação sobre a disponibilidade do dispositivo.

O outro tipo de monitorização tem por base a utilização de agentes. Os agentes são pequenas aplicações que correm nas máquinas remotas e que recolhem a informação localmente e a devolvem ao servidor monitor. A monitorização com recurso a agentes tem algumas desvantagens como o tempo que é necessário despender para instalar o agente na máquina remota e o impacto negativo que estas aplicações podem ter no desempenho da máquina onde são instaladas, mas essas desvantagens são compensadas com a possibilidade de ter o maior detalhe possível sobre a máquina remota, permitindo por exemplo ver os estados dos recursos associados aos dispositivos e o estado dos serviços da rede.

Assim, embora muitas ferramentas anunciem a auto-descoberta de dispositivos como uma das características mais importantes e diferenciadoras, o facto é que essa funcionalidade acaba por não justificar a importância que lhe é dada. É normalmente preferível ter uma maior carga na fase de configuração dos servidores de monitorização e nos dispositivos monitorizados, com a instalação dos agentes, para posteriormente se poder usufruir de uma informação mais detalhada de toda a rede.

1.3.2. Principais funcionalidades

As principais funcionalidades de um sistema deste tipo são a apresentação, quase em tempo-real, do estado actual da rede e de todos os dispositivos, recursos e serviços que a compõem, e o envio de notificações a reportar eventuais estados críticos que surjam associados a estes.

A apresentação dos dados recolhidos é geralmente feita de duas formas: no formato de tabelas organizadas ou através de gráficos personalizados. Os gráficos permitem que o administrador acompanhe o desempenho dos componentes monitorizados ao longo do tempo.

O envio de notificações é, na maior parte dos casos, personalizável e permite que o utilizador escolha qual o meio a utilizar, bem como os contactos que receberão as notificações.

Existem ainda outras características deste tipo de sistemas. Abaixo exemplificam-se algumas delas:

- Definição de horários de funcionamento dos dispositivos

- Criação de mapas de salas com identificação da localização dos dispositivos

- Comunidade de desenvolvimento de extensões para a ferramenta

À parte das características comuns, e porque a oferta de ferramentas de monitorização é bastante extensa, existem características mais restritas que funcionam como elemento diferenciador a favor de algumas das ferramentas que as disponibilizam. Um desses exemplos é a área dedicada ao *Business Intelligence*, presente em algumas delas. Esta área oferece as funções de criação e visualização de relatórios personalizados com informação sobre o comportamento da rede que podem, inclusivamente, ser enviados para os correios electrónicos dos administradores ou de outros contactos definidos como destinatários, sendo uma forma útil de reunir a informação sensível num só lugar.

1.3.3. Tipos de ferramentas de monitorização (*open-source* ou comercial)

Actualmente existem dezenas de soluções disponíveis para gestão e monitorização de uma rede. Essas soluções dividem-se em duas áreas: ferramentas públicas, ou *open-source*, e ferramentas comerciais.

Das muitas ferramentas de monitorização disponíveis no mercado, existem, felizmente, muitas delas que se apresentam como *open-source*, ou seja gratuitas e com o código fonte disponível para que qualquer pessoa possa continuar o seu desenvolvimento. Como ferramenta de monitorização de dispositivos e serviços numa rede, o Nagios é o exemplo de uma aplicação *open-source*, e uma das que tem mais utilizadores em todo o Mundo.

As ferramentas com licença comercial têm a vantagem de, na maior parte das vezes, serem mais completas a nível de oferta de funcionalidades sendo muitas vezes ideais para empresas médias ou grandes, não se justificando a sua implementação em empresas pequenas. Optar por comprar uma versão comercial de uma ferramenta de monitorização implica um custo de aquisição inicial, acrescido, por vezes, de um custo de manutenção, representando a maior contrariedade para quem deseja implementar um sistema de monitorização da sua rede e resultando num aumento de custos, precisamente o contrário do objectivo que se pretende atingir com a utilização de uma ferramenta de monitorização

As versões *open-source* costumam ser limitadas a nível de funcionalidades ou a nível do suporte, manutenção ou extensões. No que diz respeito às extensões, geralmente os utilizadores que optam pelas versões comerciais têm acesso a extensões comerciais exclusivas, embora as extensões da versão *open-source* tenham o suporte da comunidade, na maior parte dos casos tanto a nível da documentação disponível como de desenvolvimento, apresentando por isso uma grande diversidade.

A escolha de uma ferramenta de monitorização, por parte de uma empresa, deve ser feita com o objectivo de garantir a melhor relação custo-funcionalidades, tendo sempre em conta que a garantia de operacionalidade, de suporte ou de manutenção pode não ser a mesma numa aplicação *open-source* como é num produto licenciado. Porém, existem hoje em dia muitas ferramentas gratuitas que ombreiam com as pagas a nível das funcionalidades disponibilizadas.

1.4 Sistemas de apoio à decisão

Uma das características pouco comum nas ferramentas de monitorização de redes actuais é a presença de um sistema de apoio à decisão. Um sistema de apoio à decisão (SAD) é um sistema de informação que, utilizando informação obtida a partir de uma base de conhecimento (base de dados), aplicando um motor de regras a essa mesma informação e apresentando os resultados numa interface, tem como objectivo ajudar a resolver problemas ou a suportar as tomadas de decisão por parte dos seus utilizadores, qualquer que seja o sector em que este sistema seja utilizado.

1.4.1. Tipos de sistemas

Existem dois tipos diferentes de SAD, aqueles baseados em conhecimento, compostos por regras que definem quais os resultados a apresentar mediante os dados recebidos, e aqueles que não se baseiam em conhecimento, utilizando algoritmos de inteligência artificial, como as redes neuronais e os algoritmos genéticos, que permitem que o computador aprenda com a experiência passada.

1.4.2. Implementação e características

A implementação de um sistema deste tipo está muito dependente da área para a qual é desenvolvido, sendo que existem áreas mais sensíveis que outras. A área da medicina é o exemplo de uma área que lida com informação bastante sensível – a saúde dos pacientes - e onde existem actualmente alguns SAD implementados que não são porém totalmente aceites, apresentando ainda alguma controvérsia. Ainda nessa área, como exemplo, existem alguns sistemas que pretendem auxiliar o médico no diagnóstico de doenças e na prescrição de medicamentos, com base nos sintomas apresentados pelo paciente. Cabe ao médico saber interpretar, filtrar e utilizar esta informação da melhor maneira. O exemplo anterior serve para esclarecer que antes de se desenvolver ou implementar um novo SAD, é necessário analisar todos os impactos que este poderá ter, tentando obter a melhor relação custo-eficácia possível.

O debate que existe em volta deste tipo de sistemas deve-se essencialmente às diferentes interpretações sobre a melhor forma de os utilizar. Primeiro que tudo, o utilizador deve saber que um sistema deste tipo é pensado como uma ferramenta de suporte, que fornece informações que auxiliam na tomada de decisões, e nunca como uma ferramenta que fornece respostas definitivas, sob pena de se obterem efeitos colaterais indesejáveis. Depois, é necessário garantir que os dados vêm de uma fonte de conhecimento fiável, para que o sistema não apresente resultados errados, e ainda garantir uma manutenção regular desse nível de fiabilidade. Por fim, é necessário, por vezes, fornecer formação aos futuros utilizadores do SAD, para que saibam aproveitar todas as funcionalidades de um sistema deste tipo.

Outro dos requisitos no desenvolvimento de um SAD é garantir a sua integração com uma ferramenta já existente, para facilitar a interacção com o utilizador. Existem casos reais em que o SAD foi desenvolvido como uma aplicação *stand-alone*, à parte de outros sistemas essenciais para a área para a qual foi criado, dificultando assim a sua utilização.

1.4.3. Sistema de apoio à gestão

A área da gestão de redes de dispositivos é uma área onde se poderá aplicar o conceito de SAD de forma a tentar ajudar os administradores na sua tarefa de gerir a rede, identificando eventuais problemas e suportando as alterações a realizar para os eliminar. Uma das vantagens de implementar um SAD numa ferramenta deste tipo é o facto de a fonte de dados estar facilmente acessível ao sistema, geralmente no formato de base de dados, tornando o processo de apoio mais fácil e rápido de realizar.

1.5 Objectivos do trabalho desenvolvido

O interesse do autor na área das ferramentas de monitorização de dispositivos de rede motivou o desenvolvimento deste trabalho, com vários objectivos definidos e divididos por diferentes fases do desenvolvimento:

- Análise do conceito de monitorização de dispositivos
- Estudo das ferramentas de monitorização existentes
- Análise da melhor ferramenta de monitorização disponível
- Escolha de uma ferramenta para integração com nova solução
- Desenvolvimento de uma solução Web para integrar com a ferramenta escolhida
- Apresentação da nova solução de monitorização
- Comparação dos resultados obtidos com a nova solução

Este trabalho iniciou-se com a abordagem do conceito de monitorização de redes, reconhecendo-se a importância de adoptar uma ferramenta para cumprir este objectivo e estudando-se o habitual funcionamento desta. Com o estudo das ferramentas de

monitorização, o autor pretendeu tomar conhecimento do *software* desta área disponível no mercado, investigando as características de cada uma.

Após o estudo das ferramentas disponíveis, foram ponderadas e comparadas todas as características de forma a escolher a melhor ferramenta que permitisse fazer a integração com uma nova solução, ou seja, que pudesse ser usada como motor de monitorização para a nova solução a desenvolver. O desenvolvimento visou assim criar uma nova ferramenta de monitorização e configuração a partir do Nagios que oferecesse mais simplicidade que as existentes e que apresentasse novas e diferentes funcionalidades. Entre as novas funcionalidades incluiu-se o desenvolvimento de um sistema de apoio à decisão, integrado na nova solução, numa vertente de apoio à gestão de redes, possibilitando a implementação de um sistema que pudesse aproveitar melhor os dados recolhidos na rede e dotando o utilizador com algumas ferramentas que facilitassem a gestão da rede de uma empresa de diferentes formas.

A última fase deste trabalho é a apresentação da nova solução de monitorização, análise de todas as suas funcionalidades e de todos os resultados obtidos com a mesma.

Capítulo 2

Estado da Arte

Neste capítulo será analisada a evolução histórica das ferramentas *open-source* de monitorização de redes de dispositivos. Serão apresentadas as ferramentas mais importantes na área com uma visão global de cada uma delas, analisando-se os requisitos para instalação, a sua arquitectura, a sua funcionalidade e fazendo um escrutínio dos resultados obtidos com a sua utilização. Apresenta-se ainda um estudo de algumas ferramentas que utilizam a ferramenta de monitorização Nagios como motor de monitorização.

A arquitectura das ferramentas de monitorização é normalmente dividida em três camadas principais: a camada de recolha, a camada de tratamento de dados e a camada de apresentação dos dados. A comunicação necessária para se proceder à recolha dos dados é geralmente feita com recurso a agentes. A máquina onde se instala a aplicação de monitorização é capaz de detectar os estados dos dispositivos presentes na rede, sem utilizar agentes. No entanto para poder apresentar um maior detalhe dos mesmos (conhecimento dos recursos de cada máquina e dos respectivos estados) é normalmente necessária a instalação de uma aplicação agente em cada uma das máquinas remotas. Essa aplicação agente funcionará como um intermediário na comunicação entre o servidor e o dispositivo.

Como se verá, nem todas as aplicações de monitorização têm o mesmo processo para comunicação. Existem diversas formas de contactar com os dispositivos remotos, seja através da utilização de protocolos de comunicação existentes, como o SNMP ou o SSH, ou através de aplicações desenvolvidas com o objectivo específico de permitir essa comunicação. Também as funcionalidades das ferramentas variam, existindo algumas soluções mais completas que outras e por vezes demasiado complexas para o utilizador comum.

O tratamento dos dados implica normalmente o armazenamento da informação em bases de dados para posterior acesso. Há aplicações que utilizam o motor RRDTool (Round Robin Database Tool) para tal, sendo este um motor com excelentes características, particularmente na área de armazenamento de dados, pois permite evitar o escalonamento do tamanho das bases de dados e a criação de gráficos a partir dos dados que armazenou. A apresentação de todas as ferramentas analisadas é normalmente feita num portal ou interface Web.

A notificação de problemas na rede é uma das funcionalidades principais de uma ferramenta de monitorização pelo que, todas elas, de uma maneira ou outra, têm formas de avisar o utilizador sempre que necessário.

2.1 Nagios

2.1.1. Visão Global

Uma das primeiras ferramentas de monitorização *open-source* criadas foi lançada em Março de 1999 por Ethan Galstad e dava pelo nome de NetSaint [3]. Permitia monitorizar computadores, routers, impressoras e serviços de rede como o SMTP, o POP3 e o HTTP, e enviar notificações cada vez que ocorriam problemas na rede ou se recuperava dos mesmos, tudo isto de uma forma completamente gratuita. Outra das características interessantes era o conceito inovador dos *plug-ins*, pequenos *scripts* usados para fazer as verificações às máquinas remotas, que podiam ser também criados pelos utilizadores à sua medida, permitindo assim aumentar consideravelmente o leque de dispositivos monitorizáveis.

Em 2002, devido a problemas legais, o NetSaint tornou-se conhecido por Nagios [4]. Desde cedo, uma das razões para o sucesso do Nagios foi a sua extensa comunidade, responsável pelo desenvolvimento de novos *plug-ins*, *addons*, extensões e outros componentes para a ferramenta, divididos por diversas categorias e disponíveis num portal criado para o efeito [5]. Na categoria de interfaces Web, ou seja dos novos *frontends* que utilizam o Nagios como núcleo central e que, na maior parte das vezes, estendem as suas funcionalidades, surgiram desde então diversas soluções. Muitas delas acabaram por se tornar mais do que simples interfaces, tornando-se mesmo novas ferramentas de monitorização e comprovando uma vez mais a merecida notoriedade conquistada pelo Nagios. Existe também uma extensa bibliografia e documentação sobre esta aplicação de monitorização.

2.1.2. Requisitos e Instalação

Os dois principais requisitos para instalar o Nagios são um computador com um sistema operativo Unix e um compilador de C. Embora a instalação não seja um processo trivial, requerendo algum conhecimento do ambiente Unix, nomeadamente noções de como trabalhar com a consola, o suporte dado pela documentação disponível é suficiente para que rapidamente se veja a ferramenta a funcionar. É também possível instalar o Nagios numa máquina virtual, revelando-se porém uma tarefa mais árdua, dado que, neste caso, não existe documentação oficial que facilite o processo.

Após a instalação do Nagios na máquina servidora, e para que se possa monitorizar outras máquinas, é necessário instalar uma aplicação denominada de agente, responsável pela execução das verificações na máquina remota e pela consequente devolução dos resultados obtidos ao servidor de monitorização, com o qual comunica através de um *plug-in* existente neste. Este processo tem que ser realizado tantas vezes quantas as máquinas que se pretender monitorizar. Os agentes de monitorização disponíveis dividem-se em dois tipos, consoante o sistema operativo em que funcionam. A monitorização de máquinas em ambiente Unix pode utilizar um de três métodos disponíveis: monitorização por SSH, por SNMP ou através do agente NRPE. Para se monitorizar máquinas com sistemas operativos Windows, podem utilizar-se o NSClient++, o NRPE_NT ou o NC_Net. De todos os agentes referidos, os mais utilizados são o NSClient++ e o NRPE, que serão apresentados a seguir.

O NSClient++ é um agente de monitorização que funciona como um serviço, exclusivamente em máquinas com sistema operativo Windows. Esta aplicação pode funcionar em dois modos distintos. Num dos modos é utilizado um *plug-in* de nome *check_nt,* que está instalado no servidor, para pedir a informação à máquina remota.

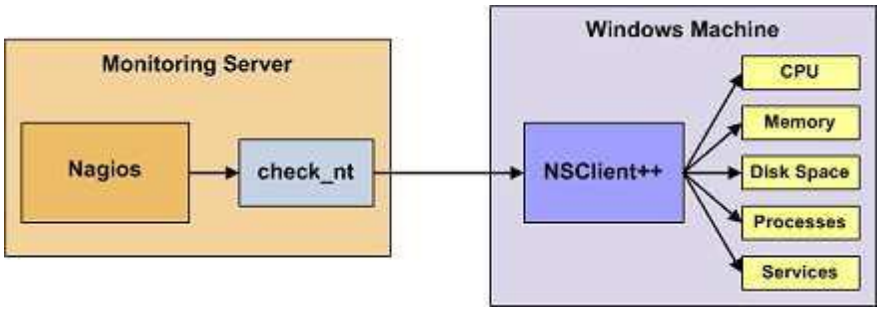

Figura 2.1 – Exemplo de monitorização com o NSClient++ num ambiente Windows

No outro modo, o agente associa-se a uma porta na máquina remota, geralmente a porta 5666, e o servidor comunica com esse serviço através da porta, utilizando para tal o *plug-in check_nrpe.*

O NRPE é um agente para monitorização remota desenvolvido pelo mesmo criador do Nagios, sendo de utilização exclusiva em ambientes Unix. Esta aplicação divide-se em dois componentes, um *plug-in check_nrpe*, instalado no servidor, e um serviço NRPE, instalado na máquina remota que se pretende monitorizar [13].

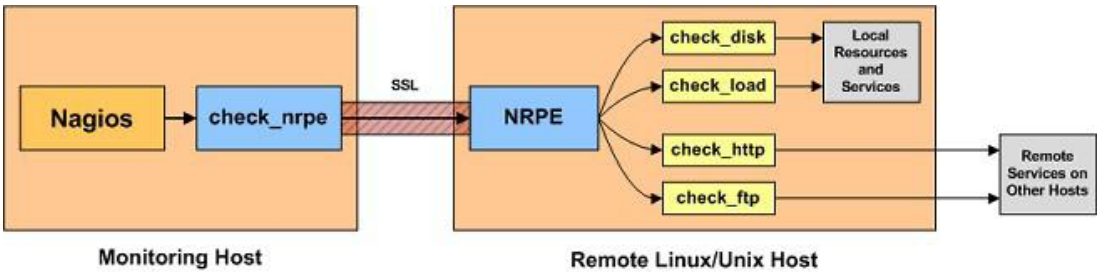

Figura 2.2 – Exemplo de monitorização com o NRPE num ambiente Unix

O *check_nrpe* envia para o serviço NRPE o nome do comando a executar na máquina remota. Por sua vez, o NRPE executa esse comando, recolhe a informação e devolve-a ao *plug-in*. Este último devolve então a informação recebida ao servidor Nagios. Esta comunicação é realizada por TCP, através da porta 5666 da máquina remota.

2.1.3. Arquitectura

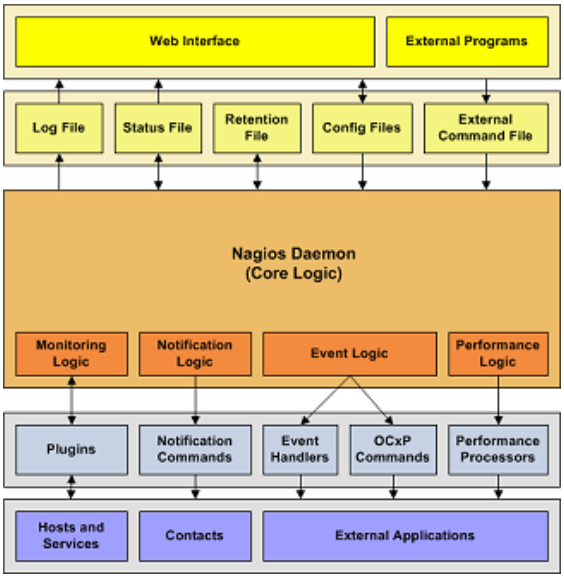

Figura 2.3 – Arquitectura do Nagios

A arquitectura do Nagios tem por base o conceito de servidor e cliente. O servidor é a máquina que está a monitorizar sendo os clientes as máquinas remotas que estão a ser monitorizadas. Pode organizar-se a arquitectura, dividindo-a em cinco níveis, estando o serviço principal do Nagios no nível central, sendo este responsável pela lógica de monitorização, de notificação, de eventos e de desempenho da rede. Abaixo deste está o nível dos *plug-ins*, dos comandos de notificações, dos *event handlers* e de outros, ou seja este é o nível de comunicação do Nagios com o exterior. O exterior é representado pelo nível mais baixo desta arquitectura, o nível onde existem as máquinas e serviços que se pretendem monitorizar, os contactos para envio de notificações e as aplicações externas que são activadas no caso de surgirem determinados eventos.

Acima do nível do Nagios Daemon estão dois níveis igualmente importantes. O primeiro é constituído pelo nível dos ficheiros de estado, de configuração e de registo, entre outros. É nestes ficheiros que é guardada toda a informação de configuração do sistema e dos dispositivos que monitoriza. Acima dele, está o nível mais alto desta arquitectura, o nível da interface Web do Nagios, que mostra a informação consoante as configurações realizadas no nível anterior e consoante a informação recebida dos *plug-ins* do segundo nível.

2.1.4. Configuração inicial

Para que seja possível ver o Nagios realizar a sua principal função – monitorizar – é necessário primeiro adicionar um novo dispositivo ao sistema. A definição deste dispositivo é feita num ficheiro de configuração pré-existente ou num novo ficheiro, com a adição de alguma informação vital para que o Nagios possa monitorizar a máquina:

- Nome da máquina

- IP ou nome da máquina rede

- Identificação da máquina no Nagios

Concluída esta fase é então possível escolher quais os serviços associados à máquina que se pretende também monitorizar. Os serviços são também definidos no mesmo ficheiro de configuração onde são definidas as máquinas a que ficam associados, para que o Nagios possa, para cada dispositivo, ler toda a informação sequencialmente.

Para que o Nagios seja actualizado com estas novas alterações, e se o mesmo já estiver sido executado anteriormente, é necessário reiniciá-lo. Completado todo este processo, o Nagios começa finalmente a monitorizar o novo dispositivo.

2.1.5. Funcionamento

O funcionamento do Nagios tem por base as verificações do estado das máquinas, dos recursos a elas associados e dos serviços públicos da rede. Com base nessas verificações podem ser detectados valores diferentes dos esperados e fora do âmbito estabelecido pelos *thresholds* pré-definidos, despoletando o envio de notificações para os administradores da rede ou de eventos que resolvam o problema de uma forma proactiva.

Toda a informação relativa à rede é apresentada numa interface Web em vários formatos, como tabelas e gráficos. É possível ver os estados de dispositivos, de recursos associados aos dispositivos e de serviços da rede que estejam a ser monitorizados. Qualquer estado crítico é observável na interface. Existe ainda um mapa de rede que permite ver a dependência hierárquica entre os dispositivos do sistema.

2.1.5.1. Verificações

O Nagios possui uma agenda das verificações que tem que executar. Essa lista pode ser personalizada pelo utilizador, sendo possível alterar a posição de determinadas verificações na lista, como por exemplo estabelecer como maior prioridade a verificação do estado da memória física de uma determinada máquina. Estas verificações podem ser realizadas a três tipos de componentes de rede, as máquinas, os recursos associados e os serviços.

Verificações de máquinas e serviços públicos

Para realizar a verificação do estado das máquinas de uma rede, o Nagios utiliza, na maior parte das vezes, o comando PING. Esta verificação pode ser feita normalmente, respeitando a sua posição na agenda de verificações ou pode ser despoletada por outras razões, como quando o estado de um serviço associado a essa máquina muda ou quando há a alteração do estado numa máquina parente, pertencente à mesma estrutura hierárquica dessa máquina.

As máquinas verificadas podem estar num de três estados possíveis:

- UP;

- DOWN;

- UNREACHABLE.

Quando uma máquina está no estado DOWN, o Nagios verifica se a máquina se encontra mesmo desligada ou se está no estado UNREACHABLE, ou seja, se está ligada mas inacessível porque uma ou mais das suas máquinas parentes se encontram no estado DOWN. Desde que haja uma alteração de estado da máquina, o Nagios poderá gerar eventos ou enviar notificações de acordo com a situação.

A nível de serviços públicos da rede, o Nagios permite ainda verificar serviços como os protocolos de gestão de correio electrónico POP3 e IMAP, o protocolo de transmissão de correio electrónico SMTP, e o protocolo de comunicação HTTP.

Verificações de serviços

A verificação de serviços é realizada normalmente de uma forma periódica, seguindo a lista de verificações estabelecida. Os serviços verificados podem estar num de quatro estados possíveis:

- OK;

-WARNING;

-UNKNOWN;

-CRITICAL.

Ao contrário das verificações de máquinas, os serviços são verificados com recurso à utilização de *plug-ins*. Consoante o resultado devolvido por estes últimos, o Nagios poderá agendar uma nova verificação à máquina à qual os serviços pertencem, enviar notificações e gerar eventos.

2.1.5.2. Plug-ins

A verificação de estados de serviços não é feita por mecanismos internos ao Nagios. Em vez disso, para que seja possível monitorizar recursos de máquinas remotas, para além de requerer a instalação de um agente na mesma, é imprescindível que se instalem *plug-ins* no próprio servidor do Nagios.

Os *plug-ins* são pequenos *scripts* corridos a partir da linha de comandos, que comunicam com o dispositivo remoto, para verificar o seu estado ou de um recurso associado, recebendo os

resultados dessas verificações directamente dos agentes aí instalados, para o Nagios. Este, por sua vez, trata os resultados e apresenta-os na interface Web.

A vantagem de se utilizarem *plug-ins* para as verificações é que se torna fácil monitorizar praticamente todos os estados das máquinas, dos seus recursos e dos serviços disponíveis na rede. Existe já uma grande comunidade à volta do Nagios, com centenas de *plug-ins* criados e disponíveis para *download*. Mesmo que o material disponível não sirva as pretensões de um utilizador, é sempre possível efectuar o desenvolvimento de um novo *plugin*, sendo essa tarefa apoiada e facilitada pela documentação e suporte existentes.

A desvantagem principal da utilização de *plug-ins* é o facto do Nagios não saber o que está a ser monitorizado. O que a aplicação faz é monitorizar e detectar apenas as alterações na informação do estado dos recursos que é recebida a partir de determinado *plugin*, agindo em conformidade.

2.1.5.3. Interface Web

Na sua versão 3.2.0, o Nagios funciona através de uma interface Web que disponibiliza várias funções de análise do comportamento e desempenho da rede. A apresentação está dividida em três áreas: a área de monitorização, a área de *reporting* e a área de configuração.

Sendo o funcionamento do Nagios baseado na monitorização e recolha de informação dos dispositivos remotos, a área principal desta ferramenta é claramente a da monitorização. Nela é possível ter uma noção do estado geral da rede e do estado individual de cada um dos seus componentes. Esta informação pode ser vista de várias formas, numa visão global, em detalhe por dispositivo ou por serviço, agrupada por grupos de dispositivos, agrupada por grupos de serviços, ou até mesmo num, não muito compreensível, mapa de estado em 2D ou 3D, que relaciona os dispositivos mediante as suas hierarquias. Também os problemas da rede têm secções dedicadas, uma para os problemas com os dispositivos e outra para os problemas com os serviços. O estado do desempenho geral da rede é também consultável nesta área, bem como a lista de verificações agendadas, onde o utilizador pode definir as prioridades para cada verificação aos dispositivos, recursos e serviços de rede.

Para uma análise mais personalizada e detalhada da informação da rede, a segunda área, a área de *reporting*, permite que o utilizador crie e visualize uma grande variedade de gráficos. É possível, por exemplo, analisar as tendências do comportamento de um determinado recurso, como o comportamento da carga de *cpu* de um computador ao longo do tempo. Para se saber quais os estados das máquinas que estão registadas no sistema, existe também a opção de criar gráficos de disponibilidade. É nesta área que se configuram ainda as notificações e se pode ver informação sobre os alertas no sistema, analisando um histograma, vendo o histórico ou um sumário dos mesmos.

O Nagios disponibiliza ainda várias opções na área da configuração do seu próprio sistema.

2.1.5.4. Modelos

Um modelo no Nagios é uma definição genérica para um tipo de objecto particular [12]. O processo de definição de novos dispositivos no Nagios pode ser um processo rápido se o número de dispositivos que se pretender monitorizar for pequeno. No caso de os dispositivos serem em grande número, a definição de cada um deles pode tornar-se um processo repetitivo. No entanto, dado que grande parte dos dispositivos partilham algumas características, é possível reduzir o tempo dispendido na configuração, recorrendo aos modelos.

A utilização de um modelo na definição de um novo dispositivo acaba por ser a herança das características definidas nesse modelo. É ainda possível criar sequências de heranças, com diferentes dispositivos a herdarem características de outros dispositivos.

Podem ser definidos três tipos de modelos: os modelos de dispositivos, os modelos de serviços e os modelos de contactos [Ver Anexo A].

2.1.6. Resolução de Problemas

Quando existem problemas ou avisos no Nagios, esta ferramenta tem duas formas de lidar com eles: através do envio de notificações para destinatários pré-definidos ou através dos *event handlers*.

2.1.6.1. Notificações

Para além de fazer a monitorização e a apresentação dos dados, o Nagios tem ainda outra funcionalidade muito importante – as notificações. Em vez de funcionar como uma mera ferramenta de apresentação de dados relativos a uma rede, o Nagios também actua na área da prevenção, tentando evitar que os problemas surjam ou se desenvolvam.

Tanto as máquinas como os serviços podem estar em vários tipos de estado. Quando uma máquina se desliga ou quando um recurso apresenta utilização excessiva, chega-se a uma situação anómala e é gerado um alerta. O Nagios procede então ao envio das notificações, previamente configuradas, pedindo que a situação seja resolvida e se evite chegar a uma situação crítica.

Os destinatários destas notificações são definidos na secção de contactos do Nagios, sendo que as notificações podem ser enviadas através de uma grande variedade de meios: por correio electrónico, por pager, por telemóvel (via SMS), por mensagem popup do Windows, por ICQ, por MSN ou por sinal sonoro, entre outros. O pacote básico de instalação do Nagios não oferece a capacidade de envio de notificações em todos os meios referidos. Muitas das opções são acrescentadas ao Nagios através da utilização de pacotes de *plug-ins* desenvolvidos para o efeito.

A utilização de notificações é essencial numa ferramenta de monitorização, sendo, no entanto, necessário ter o cuidado de definir bem a quem as enviar, com que frequência e em que circunstâncias o fazer, de forma a não as tornar um fardo para quem as recebe, quando na realidade devem ser tratadas com a maior atenção possível para que se possam evitar problemas graves na rede. Afinal de contas uma rede de dispositivos é um sistema crítico. Para garantir que esta situação não acontece, o Nagios oferece uma série de filtros pelos quais a notificação tem que passar antes de ser enviada. Esses filtros são compostos por uma série de opções personalizáveis por cada utilizador, de acordo com as suas necessidades.

2.1.6.2. Event Handlers

Os *event handlers* podem ser entendidos como uma alternativa, como um complemento às notificações ou até como poupança de trabalho para os administradores da rede. Na realidade os *event handlers* são comandos que permitem realizar acções com vista à resolução proactiva do problema, evitando o envio de notificações a requerer intervenção humana. É possível realizar vários tipos de acções, como a reinicialização de um serviço que falhou ou a reinicialização do sistema operativo que deixou de responder. Porém, é necessário ter ponderação na realização de algumas acções porque poderão ter consequências danosas, como por exemplo a reinicialização remota indesejada de um dispositivo que poderá significar a perda de um trabalho que se estava a executar.

Existem dois tipos de *event handlers*: globais actuando da mesma forma sobre máquinas ou sobre serviços, ou individuais, sobre determinadas máquinas ou serviços. O Nagios oferece ainda a possibilidade de o utilizador desenvolver os seus próprios *event handlers*, com o recurso à documentação disponível.

2.1.7. Análise dos Resultados

O Nagios apresenta-se como uma ferramenta de monitorização muito poderosa, não só a nível da própria monitorização como na área da prevenção e tratamento de problemas, sendo que relativamente à primeira existe o envio de notificações para aconselhar os administradores a resolver o problema e relativamente à segunda existem os *event handlers* que permitem a resolução pró-activa do problema, antes que este se torne mais sério, evitando contactar os administradores.

A ideia do envio de notificações para alertar para eventuais problemas, com a diversidade de meios disponíveis, é bastante útil, mas há que ter cautela na sua utilização para não enviar notificações em excesso ou para contactos errados. Felizmente o Nagios oferece uma secção de configuração de filtros a vários níveis, que permite garantir que as notificações não perdem a sua eficácia, ou são ignorados, junto dos contactos responsáveis da rede. Também os *event-handlers* deverão, como se viu, ter uma utilização ponderada para evitar consequências indesejadas.

Outra das características que torna o Nagios tão apelativo é o facto de este ser uma ferramenta bastante personalizável/configurável, permitindo que o utilizador a altere ao seu gosto para atingir os objectivos que pretende. Quase tudo no Nagios é alterável e essas alterações são facilitadas pela documentação disponível em grande quantidade e qualidade. Por outro lado a extensa comunidade oferece também um excelente suporte, não só nesta área como na área do desenvolvimento de novos *addons*, *plug-ins* e outros para o Nagios.

Outra das vantagens do Nagios é o facto da maior parte das verificações efectuadas pelo mesmo serem feitas através de *plug-ins*. Este facto abre um grande leque de hipóteses para monitorizar tudo o que é dispositivo, recurso ou serviço da rede sem qualquer problema. Mesmo que não exista um *plugin* para se monitorizar um determinado dispositivo, é possível que o utilizador desenvolva o seu próprio *script*, seja em Perl, em Shell ou outra linguagem de programação de *scripts*.

Sendo o Nagios uma ferramenta *open-source*, com o código-fonte com base no acordo de licença GPL (Gnu Public License), é ainda possível que qualquer pessoa tenha acesso ao código e faça as alterações estruturais que desejar, embora para tal sejam necessários conhecimentos prévios.

Porém o Nagios não é perfeito em tudo. Embora seja bastante personalizável, a verdade é que o processo de alteração da configuração do Nagios, do próprio sistema ou da informação dos dispositivos e serviços da rede, é bastante moroso. A interface Web não disponibiliza ferramentas de configuração do próprio sistema, pelo que todo o processo tem que ser realizado através da alteração manual dos ficheiros de configuração. Felizmente a comunidade em volta desta aplicação tem colmatado esta falha com o desenvolvimento de novas interfaces Web que facilitam essa mesma configuração.

A nível de representação gráfica do desempenho dos dispositivos, o Nagios também deixa muito a desejar. Felizmente a comunidade entra mais uma vez em jogo, com o desenvolvimento de ferramentas que apresentam esta funcionalidade bem melhor desenvolvida. Muitas vezes o Nagios é usado em conjunto com uma ferramenta de criação e visualização de gráficos, como por exemplo o Cacti ou o MRTG.

A obrigatoriedade de instalação de um agente em cada dispositivo remoto que se pretenda monitorizar é outro dos pontos negativos do Nagios. Este é um processo de rápida execução no caso de empresas compostas por poucas máquinas mas torna-se muito difícil numa empresa com um grande número de máquinas que se pretendam monitorizar.

2.2 Cacti

2.2.1. Visão Global

O Cacti é uma ferramenta *open-source* de monitorização de redes desenvolvida em PHP e MySQL por Ian Berry, com a primeira versão lançada em Novembro de 2001, e tem como

principal característica a sua capacidade de criação de gráficos de desempenho de recursos [6].

O funcionamento do Cacti divide-se em três fases: a recolha, o armazenamento e a apresentação de dados. A recolha dos dados de dispositivos remotos é realiza recorrendo à utilização de uma aplicação que executa essa tarefa de tempo a tempo, designada por *poller*. A comunicação remota é realizada através do protocolo SNMP.

As restantes fases do funcionamento assentam no motor RRDTool, uma solução *open-source* que permite fazer o armazenamento dos dados e a criação de gráficos. A opção de adoptar este motor para realizar essas tarefas é acertada, dado que o RRDTool tem a característica de não aumentar muito a carga resultante do excesso de informação armazenada.

A apresentação do Cacti ao utilizador é feita através de uma interface Web que disponibiliza uma série de funcionalidades, entre as quais:

- Adição de novos dispositivos
- Visualização do estado dos dispositivos da rede
- Criação e gestão de gráficos
- Gestão de utilizadores

No geral esta solução de monitorização acaba por funcionar apenas como uma interface gráfica do excelente motor RRDTool.

2.2.2. Requisitos e Instalação

O Cacti funciona preferencialmente em ambientes Unix mas também pode ser executado em ambientes Windows. É necessário, porém, cumprir outros requisitos, garantindo a instalação prévia das seguintes aplicações:

- RRDTool;
- MySQL;
- PHP;
- NET-SNMP;
- Servidor Web (Apache ou IIS).

O motor *RRDTool* tem como função a recolha de informação das máquinas remotas e criação de gráficos sendo o MySQL utilizado para as bases de dados, o PHP para tornar possível a interface do Cacti e sendo ainda necessária a instalação de um servidor Web de entre dois possíveis, o Apache ou o IIS. Opcionalmente, também pode ser requerido o Net-SNMP para possibilitar a recolha de informação de máquinas remotas com o *RRDTool*.

A instalação do Cacti num sistema operativo Linux é realizada através da consola do mesmo e consiste nas instalações individuais de cada uma das dependências assinaladas. A instalação da ferramenta em si, poderá ser realizada de duas formas diferentes: por pacote binário ou pela *source*. A primeira opção é a mais *user-friendly*, não garantindo no entanto que a instalação a realizar seja da última versão da ferramenta. A segunda opção permite ter um maior controlo sobre a instalação, mas é apenas indicada para os utilizadores que estejam à vontade com sistemas Linux.

A instalação em Windows é feita de forma mais facilitada, bastando para tal instalar todo o software necessário, que por norma têm GUI (Graphical User Interface) que facilitam a instalação, e ter algum conhecimento do funcionamento do servidor IIS. Depois basta instalar o Cacti na pasta do servidor, para que possa ser acedido a partir do browser.

2.2.3. Arquitectura

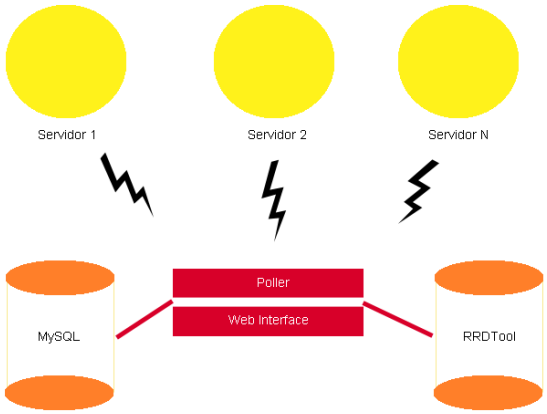

Figura 2.4 – Arquitectura do Cacti

A arquitectura da ferramenta centraliza-se essencialmente na ferramenta RRDTool, sendo o Cacti considerado um *frontend* desta que pode ser dividida em três camadas: a camada da recolha, a camada dos dados e a camada do utilizador.

Na camada de recolha, o *poller* tem a tarefa de recolher a informação dos dispositivos remotos periodicamente, sendo executado através do *scheduler* do sistema operativo (no Linux é o *crontab*). Para que isto seja possível, o tipo de comunicação utilizado entre o servidor de monitorização e os servidores monitorizados é o protocolo SNMP.

Os dados recolhidos são posteriormente passados para uma camada de dados onde são tratados e armazenados numa base de dados com recurso à ferramenta RRDTool.

Finalmente existe a camada do utilizador que permite o acesso ao sistema Cacti. A partir de uma interface Web, é possível visualizar e alterar configurações e, principalmente, utilizar todo o potencial do RRDTool para criar as mais variadas representações gráficas dos dados que foram recolhidos.

2.2.4. Configuração Inicial

O primeiro passo para usufruir das funcionalidades principais do Cacti é realizar a sua configuração inicial. Antes de criar qualquer tipo de gráfico é necessário adicionar um dispositivo, sendo para tal obrigatório definir vários atributos, o seu nome ou IP na rede, o modelo de dispositivo que vai usar e uma descrição deste dispositivo como identificação.

A segunda fase desta configuração consiste na personalização das opções de disponibilidade e acessibilidade, ou seja, as opções que caracterizam o método que o sistema vai utilizar para verificar o estado dos dispositivos. É possível escolher uma série de características para o PING e para o SNMP.

Consoante o modelo de dispositivo que se escolheu na primeira fase da configuração, é possível que já existam por defeito alguns modelos de gráficos associados e que seja possível visualizar gráficos no imediato. Caso contrário, é possível criar um de raiz.

2.2.5. Funcionamento

O Cacti é muitas vezes designado como o *frontend* do RRDTool. De facto a ferramenta RRDTool desempenha um papel crucial no funcionamento da aplicação de monitorização, sendo responsável por duas das principais tarefas do Cacti e permitindo ainda a existência de bastantes funcionalidades acessíveis a partir da interface. O Cacti acaba por ter como finalidade principal a criação de gráficos que representam o comportamento da rede ao longo do tempo.

2.2.5.1. Organização de Gráficos

A característica principal do Cacti é, sem dúvida alguma, a apresentação da informação recolhida em formato gráfico, e é aqui que reside o potencial desta solução. Entre outras funções, esta ferramenta oferece uma excelente organização dos gráficos de cada dispositivo, estando distribuídos, hierarquicamente, em árvores de gráficos.

Constituição de uma árvore de gráficos

Uma árvore de gráficos apresenta-se dividida em cabeçalhos ou nós de ramos e cada um destes ramos possui informação escondida, designada de folhas. É também possível implementar estruturas mais complexas, criando árvore de gráficos dentro de uma só árvore.

O nome da árvore identifica, geralmente, um dispositivo. Cada nova árvore ou ramo associados à árvore principal, designados de objectos parentes, representam informação relativa ao próprio dispositivo ou relativa a recursos associados ao mesmo, como por exemplo espaço em disco disponível na partição *sda1* do computador X.

Na criação de uma árvore há ainda a possibilidade de personalizar a sua disposição, escolhendo a ordem pela qual a informação é apresentada, dos quatro tipos disponíveis:

- Ordenação manual;

- Ordenação alfabética;

- Ordenação numérica;

- Ordenação natural.

Na ordenação manual é possível escolher as posições dos novos dispositivos na árvore ou nos ramos. Na ordenação alfabética, tal como o nome indica, todas as entradas são ordenadas alfabeticamente. Na ordenação numérica, cada dispositivo é ordenado numericamente. Por fim na ordenação natural é utilizada a ordenação alfanumérica.

2.2.5.2. Criação dos gráficos

Depois de configurada toda esta informação, é possível ver os gráficos com a informação relativa ao dispositivo e aos seus recursos, num total de seis em simultâneo no ecrã. A apresentação gráfica é personalizável com a escolha da data para visualização, sendo possível definir períodos para a apresentação dos dados.

2.2.5.3. Modelos

Para tornar a fase de configuração mais rápida, o Cacti também oferece o conceito de modelo. Os modelos são uma maneira de aproveitar as características comuns entre dispositivos do mesmo tipo, para que seja possível tornar o processo de definição de novos dispositivos mais rápido.

É possível utilizar e criar três tipos de templates diferentes:

- Modelos de dados;

- Modelos de gráficos;

- Modelos de máquinas.

Enquanto os dois primeiros tipos têm como função definir parâmetros indispensáveis à criação de ficheiros do tipo *rrd* (é a partir destes ficheiros que o RRDtool cria os gráficos), os modelos de máquinas não estão de todo relacionados com a ferramenta RRDtool. São sim responsáveis pelo agrupamento dos modelos de gráficos com os tipos de consultas de dados feitas a um determinado dispositivo.

Modelos de dados

A criação de um modelo de dados permite definir uma base comum para fontes de dados que partilhem características. Tome-se como exemplo a informação da utilização do CPU. Este é um recurso que é necessário monitorizar em bastantes dispositivos numa rede, como tal faz sentido criar um modelo de dados para a utilização do CPU, para que todos os ficheiros *rrd* de utilização de CPU o utilizem.

Criação de um novo modelo de dados

Um novo modelo de dados tem que ter um nome, não necessariamente o nome da fonte de dados que o utilizará. Depois segue-se a definição das características da fonte de dados. Aqui é necessário atribuir um nome à fonte de dados, definir o modo como o Cacti vai recolher os dados da fonte, por exemplo por SNMP, e ainda definir o tempo máximo que o RRDTool irá guardar os dados:

- Diariamente (média de 5 minutos)
- Mensalmente (média de 2 horas)
- Semanalmente (média de 30 minutos)
- Anualmente (média de 1 dia)

As fontes de dados poderão ser constituídas por vários objectos, de forma a poder utilizar apenas um modelo para diferentes resultados vindos da fonte de dados, como por exemplo a memória utilizada e a memória livre num dispositivo.

Modelos de gráficos

A criação de um novo gráfico pode tornar-se um processo bem mais rápido com a definição de um modelo de gráficos. Esse modelo permite definir características inerentes a vários tipos de gráficos. A primeira fase na criação do modelo é composta pela atribuição de um nome que o identifique e pela definição das características que o gráfico herdará quando utilizar este modelo, como por exemplo:

- Título
- Formato da imagem gerada
- Comprimento e altura da imagem
- Limites máximo e mínimo dos eixos
- Opções da escala

Na maior parte dos campos de configuração do modelo é possível activar uma opção para que o valor do campo seja pedido ao utilizador no momento da criação do gráfico, sendo indispensável por exemplo para a definição do título do gráfico.

A segunda fase permite definir a fonte de dados, as cores utilizadas para as legendas e para o gráfico, o formato do texto, entre outras opções.

Modelos de máquinas

A criação de um modelo de máquinas está dividida em duas partes. Primeiramente define-se o nome do modelo e escolhem-se quais os modelos de gráficos a associar ao modelo de máquinas. Depois basta associar um ou mais tipos de consultas de dados.

2.2.5.4. Importar e exportar modelos

É possível que o utilizador não precise de criar modelos, isto porque já existem vários modelos criados que poderão servir as suas necessidades. Isto só é possível porque o Cactis tem uma comunidade grande que vai desenvolvendo e partilhando, entre outras coisas, os seus modelos. A importação de um modelo pode ser feita a partir de um ficheiro XML ou então colando o código respectivo numa interface desenvolvida para o efeito.

Se por outro lado o utilizador pretender partilhar o seu modelo, é possível fazer a exportação do mesmo. Os modelos exportáveis são os de dados, gráficos ou máquinas. É também possível exportar consultas de dados. A exportação pode ser feita de três diferentes maneiras:

- Para uma interface do Cacti
- Para o browser como ficheiro XML
- Gravando o ficheiro

2.2.5.5. Gestão de utilizadores

O Cacti apresenta um complexo, mas interessante, sistema de permissões para utilizadores. É possível definir permissões diferentes para diferentes utilizadores, de forma a filtrar o acesso à informação disponível na interface. As permissões são divididas em dois grupos principais, as permissões de domínio e as permissões de gráficos.

As permissões de domínio controlam quais as secções a que os utilizadores têm acesso na interface gráfica do Cacti, destacando-se de seguida algumas delas:

- Administração de utilizadores
- Visualização de gráficos

- Actualização de árvores de gráficos, de gráficos e de fontes de dados

- Importar e exportar dados

As permissões de gráficos controlam essencialmente o acesso à visualização de informação com base em quatro tipos de filtros, por gráfico, por dispositivo, por modelo de gráfico e por árvore de gráfico. Assim é possível, por exemplo, negar o acesso a gráficos que estejam associados a uma determinada máquina ou a um modelo gráfico.

O utilizador pode ainda ter permissão para alterar as configurações dos gráficos que visualiza. Entre essas configurações, é possível controlar o tamanho do gráfico, a fonte utilizada para as legendas e o título do gráfico.

Do ponto de vista do administrador existem várias opções para além da gestão de permissões de utilizadores. Copiar, apagar, activar e desactivar utilizadores são outras das funcionalidades disponíveis, destacando-se a função de cópia de lote (*batch copy*) que permite definir um utilizador, que já tenha as suas permissões designadas, como um modelo de utilizadores e posteriormente aplicar este último a um novo utilizador. Poupa-se assim tempo na definição de novas permissões para outro utilizador e facilita as actualizações de utilizadores em massa.

2.2.6. Análise dos Resultados

O facto de funcionar sobre o RRDTool dota o Cacti de um potencial muito grande, aproveitando as exímias características de armazenamento e apresentação de dados dessa aplicação. Aliás, o Cacti caracteriza-se mesmo por ser uma ferramenta de monitorização com fortes alicerces na área de representação de dados, oferecendo várias opções de personalização dos gráficos, como a opção de definir diferentes fontes de dados para gráficos diferentes. Ainda neste plano destaque para o conceito de árvore de gráficos que permite criar hierarquias, aumentando o nível de organização com a definição de relações entre os gráficos de um mesmo dispositivo.

O ponto forte do Cacti, porém, acaba por também fazer parte da sua maior fraqueza – ser apenas orientado para apresentação de dados. Ao contrário do Nagios e do Zenoss, esta ferramenta peca pela falta de um sistema de notificações e de tratamento de erros, existentes nas duas primeiras. Com esta solução é possível ver todo o tipo de gráficos, perceber pelos mesmos que algo não está bem na rede, mas impossível fazer algo para o corrigir. Faltam os avisos na interface Web, as notificações e eventos para tratar os problemas – funções imprescindíveis numa ferramenta de monitorização e requisitos básicos para os utilizadores das mesmas.

A recolha de dados, à semelhança do Nagios, necessita da instalação de um agente na máquina remota. No Cacti esse agente é um agente SNMP. Embora represente uma maior carga na configuração da rede, esse processo é imprescindível para se ter um maior detalhe na informação desta.

A opção de criação ou importação de modelos é igualmente importante, dado que possibilita diminuir o tempo do processo de definição de novos dispositivos, tornando-o bem mais rápido e fácil para qualquer utilizador.

No que diz respeito à instalação do Cacti, dado que é necessário instalar vários componentes, como o MySQL, o PHP e o RRDTool, pode tornar-se um pouco complexa e demorada, principalmente quando a instalação é feita em ambientes Linux. Porém a configuração de novos dispositivos é facilitada pela interface Web que permite não só alterar como adicionar novas máquinas, sendo esta uma grande vantagem em relação ao Nagios que só possibilita a configuração dos dispositivos com a alteração manual dos ficheiros de configuração, fora do ambiente da interface Web.

Outra vantagem do Cacti é que pode ser executado em dois ambientes distintos como o são o Linux e o Windows, oferecendo uma documentação de suporte suficiente para os dois.

Mais do ser utilizado como ferramenta de monitorização independente, o Cacti acaba por ser muitas vezes adoptado como solução conjunta com o Nagios, utilizando-se o primeiro para configuração da rede e representação gráfica, e o último para a detecção de problemas e envio de notificações. Porém a integração destas duas ferramentas não é totalmente vantajosa para o utilizador já que acabam por funcionar através de duas interfaces distintas, quando poderiam funcionar apenas numa única.

2.3 Zenoss

2.3.1. Visão Global

Em Novembro de 2006, a empresa formada por Erik Dahl e Bill Karpovich, lançou a primeira versão do Zenoss Core, a versão *open-source* de uma ferramenta de monitorização de redes. Para além das habituais funções básicas, esta ferramenta surgia com uma característica que se diz ser inovadora, a função de auto-descoberta de dispositivos numa rede, e ainda com a compatibilidade com o formato de *plug-ins* do Nagios, numa clara manobra de sedução dos utilizadores deste último. Esta solução oferecia ainda os seus próprios *plug-ins*, as extensões chamadas ZenPacks, com suporte para o desenvolvimento da comunidade. A par da versão Core, foi também lançada uma versão paga, a Enterprise, que tinha algumas diferenças em relação à primeira, a oferta de mais suporte à ferramenta, mais funções de monitorização e o acesso exclusivo a extensões comerciais.

2.3.2. Requisitos e Instalação

A instalação do Zenoss pode ser realizada em sistemas operativos distintos, em Windows ou Linux. A instalação em Linux pode ser feita através do ficheiro binário ou pelo código fonte, requerendo a instalação prévia de todas as dependências, o MySQL e o Python, e necessitando um conhecimento básico do funcionamento da consola em Linux. A instalação

do Windows não requer a instalação das dependências, dado que é feita com base numa imagem que será executada numa máquina virtual que virá já com as dependências incluídas no pacote. Os requisitos para se poder executar esta imagem são uma máquina com processador Dual Core, um mínimo de 1.5GB de memória e um mínimo de 4GB de disco rígido livre. Em qualquer dos casos é necessário instalar o NET-SNMP, um software que cria o suporte para o protocolo SNMP na máquina onde é instalado, tanto no servidor do Zenoss como nas máquinas remotas que se pretende monitorizar, e ainda definir regras para abertura de portas nas *firewall* para possibilitar a comunicação.

2.3.3. Arquitectura

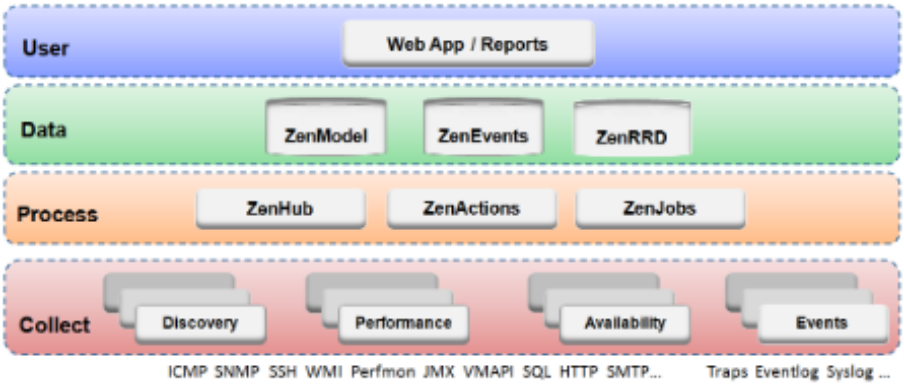

Figura 2.5 – Arquitectura do Zenoss

A arquitectura do Zenoss é divida em quatro camadas, a do utilizador, a dos dados, a dos processos e a de recolha. De seguida faz-se uma descrição breve desta arquitectura.

2.3.3.1. Camada de Recolha

A camada mais baixa da arquitectura é a camada de recolha. É composta por diversos *daemons*, ou serviços, que são responsáveis pelas funções de modelação, ou seja a recolha de dados por SNMP, SSH e WMI (este último apenas em Windows), de monitorização, ou seja a verificação do estado e do desempenho dos dispositivos, e da gestão de eventos. É nesta camada que é implementado a característica de auto-descoberta de dispositivos do Zenoss.

2.3.3.2. Camada de Processos

Esta camada é responsável por garantir a comunicação entre a camada de recolha e a camada de dados. A comunicação é feita com recurso a um sistema RPC bi-direccional.

2.3.3.3. Camada de Dados

Esta camada é composta por três bases de dados onde é guardada a configuração do Nagios e a informação recolhida na camada de recolha. Os dados de desempenho são guardados na base de dados ZenRRD, utilizando a ferramenta RRDTool. A base de dados ZenModel, guarda a informação de todos os dispositivos na rede. Os dados de eventos são guardados numa base de dados MySQL, designada por ZenEvents.

2.3.3.4. Camada de Utilizadores

A camada de topo nesta arquitectura é a camada de utilizadores. Esta camada permite a comunicação entre o Zenoss e o utilizador, através de uma interface Web desenvolvida em Ajax. A partir desta é possível aceder a toda a informação relativa à rede, gerir dispositivos, criar relatórios, entre outras opções.

2.3.4. Configuração inicial

Para que seja possível executar o Zenoss pela primeira vez, é necessário configurar o servidor que monitoriza e os dispositivos que se pretende monitorizar, também uma primeira vez. O servidor tem que ter portas da *firewall* específicas abertas, para aceitar ligações, e os dispositivos remotos têm que ter outras portas das *firewalls* abertas, nomeadamente para que o servidor aceda por SNMP e/ou por SSH.

Dado que o Zenoss utiliza o protocolo SNMP para fazer as verificações nos dispositivos remotos, é necessário que estes suportem esse mesmo protocolo. Para tal é necessário instalar um agente SNMP, nomeadamente através do software NET-SNMP, tanto no servidor com o Zenoss como nos dispositivos a monitorizar. Quando as máquinas remotas são servidores Windows e se pretende ver a informação sobre serviços e eventos Windows, é ainda necessário activar o protocolo WMI (Windows Management Instrumentation), exclusivo desse sistema operativo.

Para além da configuração inicial, o Zenoss tem ainda uma secção designada por Configurações do Sistema, onde é possível alterar toda esta informação relativa aos protocolos suportados individualmente em cada máquina.

Posto todo este processo, é então possível usufruir das funcionalidades do Zenoss, a partir da sua interface Web.

2.3.5. Funcionamento

O Zenoss divide o seu funcionamento por *daemons* em Unix, o equivalente aos serviços no Windows. Existem *daemons* para gerar eventos, sejam eventos de PING, SNMP ou de

processos, para recolher eventos, como o zensyslog para as mensagens syslog, ou *daemons* para monitorizar a disponibilidade de dispositivos através do comando PING, como o zenping, entre outros.

O funcionamento do Zenoss começa pela auto-descoberta de novos dispositivos na rede ou nas sub-redes definidas na aplicação. A função de auto-descoberta permite passar a carga do trabalho de inserção de novos dispositivos, normalmente associada ao utilizador, para a ferramenta. Para o utilizador basta definir uma gama de endereços IP na qual existem dispositivos que pretende monitorizar e posteriormente o processo de descoberta percorre cada um desses endereços, adicionando todos os dispositivos que respondem a um pedido *ICMP*. Está também disponível a opção de adicionar um novo dispositivo manualmente.

2.3.5.1. Modelação de dispositivos

Nesta ferramenta existe o conceito de modelação de dispositivos. Esta modelação consiste na identificação dos vários componentes que constituem cada dispositivo presente numa rede. Esses componentes podem ser interfaces, como por exemplo uma placa de rede que é identificada pelo seu nome e pelo seu endereço físico MAC, podem ser processos, ou seja aplicações executadas no sistema operativo como por exemplo o processo *mysqld*, podem ser serviços, sejam serviços de Windows (*ftp*, *telnet*, entre outros) ou *daemons* de Unix (*syslogd*, *sshd*, entre outros), podem ser sistemas de ficheiros, como discos rígidos ou discos amovíveis, e podem ainda ser as tabelas de encaminhamento para cada um dos dispositivos.

A modelação dos dispositivos é realizada com recurso a um variado número de protocolos, possibilitando a identificação de uma grande variedade de componentes e a recolha de informação dos mesmos. Para a identificação são utilizados o SNMP, o SSH, o WMI e o Telnet. A recolha da informação, por sua vez é feita com recurso aos *plug-ins* de recolha existentes em SNMP e SSH. Existem tantos *plug-ins* como os componentes que se pretendem monitorizar nos dispositivos.

O protocolo SNMP acaba por ser o mais utilizado mas se o dispositivo monitorizado não suportar a sua utilização, ou se existir uma *firewall* no seu caminho, existe uma alternativa para este processos - o SSH. A razão para a preferência do SNMP reside no facto do SSH nem sempre possibilitar a recolha de informação tão detalhadamente como o SNMP permite. No entanto, na ausência do SNMP, o protocolo SSH é a melhor alternativa, bastante superior à simples e pouco segura verificação dos serviços que estão a ser executados num determinado dispositivo com base na análise de todas as portas deste, método este designado de modelação por *port scan*.

2.3.5.2. Interface Web

Uma vez estabelecida a estrutura de uma ou mais redes, é possível configurar ou aceder à informação recolhida através de uma interface Web, com várias funcionalidades disponíveis.

Esta interface oferece um nível de personalização elevado, com uma apresentação composta por várias janelas, designadas de *portlets*, cuja posição no *dashboard* pode ser escolhida pelo utilizador.

Portlets

Um dos *portlets* mais interessantes é o *portlet* de localização, que utiliza o *Google Maps* para mostrar não só a posição geográfica dos dispositivos configurados como as ligações entre eles. A visualização dos problemas pode ser feita no *portlet* de problemas, onde os problemas são divididos em duas áreas, os problemas nos dispositivos da rede e os problemas no próprio Zenoss. Para se verificar o estado de um dispositivo, de uma hierarquia ou de toda a rede, está também disponível um *portlet*. De referir ainda o *portlet* de produção. Através dele é possível definir estados de produção para cada um dos dispositivos – Em Produção, em Pré-Produção, em Teste, em Manutenção e Desactivado - revelando-se uma funcionalidade bastante útil para o meio empresarial.

Classes

A nível organizacional, o Zenoss possui um conceito imprescindível, as classes. Uma classe permite agrupar objectos que partilham características comuns atribuindo-lhes uma configuração igual. Existem classes de eventos, de dispositivos, de serviços, de processos e de produtos.

Os membros de uma classe partilham eventos, propriedades e modelos de desempenho. Estes modelos de desempenho permitem definir métodos comuns, através dos quais o Zenoss recolhe os dados de desempenho dos dispositivos membros da classe.

É ainda possível criar relações parentais entre dispositivos, definindo as heranças. Um exemplo de uma herança pode ser uma firewall pertencer a um grupo de routers, que por sua vez pertence ao grupo geral da rede.

2.3.5.3. Gestão de dispositivos

O Zenoss oferece uma extensa secção de gestão dos dispositivos da rede. Para além de ser possível ver o estado global da rede e individual de cada componente da rede, é possível executar uma série de funções relacionadas com a alteração das configurações dos dispositivos, como por exemplo adicionar um novo dispositivo, de uma maneira mais personalizada e bem diferente do que a funcionalidade de auto-descoberta permite, renomear, alterar o endereço IP ou apagar um dispositivo existente. Para que estas alterações em vigor ou se espera que o Zenoss as actualize no sistema ou utiliza-se uma função que faz a actualização no imediato.

Uma das propriedades interessantes desta gestão é a possibilidade de fazer uma actualização em massa, ou seja proceder a alterações de configurações de vários dispositivos ao mesmo tempo.

2.3.5.4. Gestão de Eventos

O Syslog é um protocolo que permite que um dispositivo envie mensagens de notificação para colectores de mensagens, designados por servidores ou *daemons* Syslog, sempre que há uma alteração na sua configuração ou funcionamento.

Cada vez que existe um problema na rede, seja um recurso com excesso de utilização, ultrapassando um determinado *threshold*, ou um dispositivo que simplesmente deixou de responder, o Zenoss cria um evento para enviar uma notificação.

Para dispositivos baseados em Unix, o Zenoss aproveita a potencialidade do Syslog e utiliza o seu *daemon* zensyslog para receber as mensagens syslog desses dispositivos, e a partir delas, cria eventos que acabam por ser notificações dos problemas identificados. No que diz respeito aos dispositivos baseados em Windows, para monitorizar o *log* de eventos do dispositivo é necessário haver uma ligação ao servidor Windows.

Através da interface Web é possível aceder a um gestor de eventos que possibilita personalizar o seu funcionamento, o seu armazenamento e a forma como são visualizados.

2.3.5.5. Gráficos de desempenho

Para analisar o comportamento de uma rede ao longo do tempo, o Zenoss também disponibiliza a criação de gráficos com base no desempenho dos componentes que monitoriza. Para guardar esta informação de desempenho ao longo do tempo, é utilizado o RRDtool.

É possível visualizar gráficos de desempenho de vários elementos, entre estes os pacotes recebidos numa placa de rede (interface), a carga de utilização de um CPU, a memória em uso e a utilização de um disco rígido. Existem diferentes escalas do tempo para visualização dos gráficos, podendo ser vistos por hora, diariamente, semanalmente, mensalmente ou anualmente.

A personalização dos gráficos é outra das opções disponíveis, permitindo que se alterem as definições dos mesmos. Podem alterar-se as fontes de dados, as unidades a apresentar no eixo das ordenadas, o tamanho da imagem do gráfico e a sequência pela qual são apresentados.

2.3.5.6. Relatórios

No Zenoss a visualização da informação da rede, incluindo as relações entre os seus dispositivos, e a apresentação do desempenho do seu comportamento, é realizada com base em relatórios. Existe uma grande variedade de relatórios disponível:

- Relatórios de dispositivos;
- Relatórios de eventos;
- Relatórios gráficos e multi-gráficos;
- Relatórios de desempenho;
- Relatórios de utilizadores.

Relatórios de dispositivos

Os relatórios de dispositivos são compostos por vários relatórios que permitem ver todas as informações referentes aos dispositivos da rede. Esses relatórios são organizados no formato de tabelas e no geral os dispositivos são distinguidos pelo seu nome, pela classe a que pertencem, pelo estado em que se encontram, bem como pelos valores devolvidos pelas verificações feitas por PING e por SNMP.

Ainda nesta secção é possível ver relatórios de todos os componentes monitorizados pelo programa, desde serviços de rede, a processos, interfaces e sistemas de ficheiros.

Qualquer alteração realizada num dispositivo ou qualquer adição de um novo dispositivo na rede é registada no sistema, sendo possível visualizar relatórios referentes às mesmas. O Zenoss possui ainda um interessante sistema de inventário que organiza o *software* instalado nos dispositivos, por fabricante e por número de programas instalados.

Relatórios de eventos

Os relatórios de eventos possibilitam ver a informação referente às classes de eventos existentes e o estado dos *daemons* do Zenoss associados.

Relatórios gráficos

Os relatórios de gráficos permitem juntar múltiplos gráficos que estão relacionados entre si por representarem dados de diferentes dispositivos mas comuns entre estes. Por exemplo, se o utilizador pretender visualizar a utilização do CPU em todos os servidores, é possível criar um relatório que mostre a utilização de CPU individual de cada um dos servidores, todos ao mesmo tempo. Contudo existe uma limitação a notar, este tipo de relatórios só apresentam

gráficos, de dispositivos ou componentes no sistema, que já existem, não sendo possível definir novos gráficos ou proceder a alterações aos já existentes. Esta limitação é ultrapassada com recurso aos relatórios de múltiplos gráficos.

Um relatório de múltiplos gráficos permite a definição das fontes de dados para a criação de novos gráficos e permite ainda a criação de um único gráfico composto pela informação referente a vários dispositivos ou componentes – uma colecção.

Relatórios de desempenho

Os relatórios de desempenho permitem observar o desempenho dos dispositivos e componentes da rede, ao longo do tempo. Para cada dispositivo ou componente é possível ver:

- A informação da disponibilidade na rede
- A carga média e a percentagem de utilização do CPU
- Informação da utilização dos sistemas de ficheiros
- Informação da utilização da interface de rede
- Informação da utilização da memória física

É também possível utilizar os chamados relatórios agregados que permitem que se veja o desempenho combinado de um determinado componente, por exemplo a memória física, para todos os dispositivos, o que é ideal pois permite criar fazer uma análise comparativa de um recurso entre todos eles e ter uma ideia geral do comportamento da rede em determinado período. Existe ainda um relatório que permite visualizar todos os dispositivos que ultrapassaram os *thresholds* de desempenho estabelecidos.

Relatórios de utilizadores

Igualmente importantes são os relatórios de utilizadores que permitem definir relatórios de agendamento de notificações para cada um dos utilizadores registados no Zenoss, mostrando as regras, o estado e a duração dos alertas.

Uma das vantagens deste complexo sistema de relatórios é a possibilidade de exportar a informação de qualquer relatório para um ficheiro do tipo *csv*, permitindo que seja lido noutros programas, como por exemplo o Microsoft Excel.

2.3.5.7. Gestão de utilizadores

Esta ferramenta oferece uma boa gestão de utilizadores, possibilitando definir privilégios de acesso à interface diferentes, associar regras de alerta individuais, entre outras opções.

As regras de alerta são associadas aos utilizadores e tornam possível que os eventos resultem em acções que resolvam os problemas que os originaram. O envio é feito via SMTP, por correio electrónico, ou SNPP (Simple Network Paging Control), um protocolo que permite definir um método pelo qual um *pager* pode receber mensagens pela Internet. Outro ponto interessante é a possibilidade de criar uma hierarquia de alertas. Se, por exemplo a primeira pessoa, assuma-se a pessoa A, que tem que responder a alertas na hierarquia, não o fizer, então a pessoa B, a seguinte na hierarquia, é notificada para responder. Assim há uma maior probabilidade de serem resolvidos todos os problemas na rede.

2.3.5.8. Janelas de Manutenção

Uma característica interessante do Zenoss é a possibilidade de definir janelas de manutenção para os dispositivos, ou seja definir períodos em que os dispositivos ficam marcados como ausentes com o conhecimento da rede e, como tal, enquanto se mantiverem nesse estado, a ferramenta não os monitoriza nem alerta para eventuais problemas nos mesmos. Esta função é semelhante aos *timeperiods* no Nagios.

2.3.5.9. ZenPacks

À semelhança do Nagios, o Zenoss tem um mecanismo de personalização e extensão das próprias capacidades, designado por ZenPacks. O ZenPack permite adicionar variados componentes ao Zenoss, como por exemplo comandos do utilizador, novas classes de serviço, modelos para criação de gráficos, novos tipos de relatórios e novos menus para a interface. A criação destes pacotes pode ser feita na própria interface Web do Zenoss ou então com base em desenvolvimento de *scripts* ou *daemons*, uma opção mais complexa mas que permite uma maior variedade e criatividade na fase de criação.

Os ZenPacks são um dos elementos diferenciadores das características das duas versões do Zenoss que estão disponíveis, a Core e a Enterprise, existindo diferentes pacotes nestas duas versões. Com qualquer uma destas versões instaladas, porém, é possível utilizar outro tipo de ZenPacks, os desenvolvidos pela comunidade.

2.3.6. Resolução de Problemas

No Zenoss quando surge alguma anomalia nos dispositivos monitorizados, como por exemplo quando a memória física ultrapassa um determinado *threshold*, é gerado um evento. Com base no evento gerado existem duas opções a realizar. O programa poderá actuar no plano

preventivo, gerando alertas e enviando-os por correio electrónico ou *pager*, podendo estes serem personalizados através da definição de regras, associando diferentes alertas por utilizador, ou então poderá actuar no plano correctivo, correndo comandos em *scripts* de forma a resolver o problema assim que ele surja, semelhante aos *event handlers* no Nagios.

2.3.7. Análise dos Resultados

Os requisitos para funcionamento do Zenoss podem representar um entrave à eventual implementação do mesmo. A instalação em Windows apresenta uma grande limitação, o facto de ser indispensável ter um servidor potente para executar a máquina virtual, sendo que com este método de instalação só é possível monitorizar um número reduzido de dispositivos numa rede. A instalação em ambiente Unix requer que o utilizador tenha um bom entendimento do funcionamento deste sistema operativo, particularmente com a consola do sistema.

Uma das características interessantes do Zenoss é a opção de auto-descoberta de dispositivos numa rede, embora na prática acaba por ser simplesmente a utilização do comando PING para testar a comunicação entre máquinas, verificando a sua disponibilidade. Seria desejável que essa auto-descoberta englobasse também a detecção dos recursos dos dispositivos e dos serviços da rede automaticamente, mas a realidade é que para que isto seja possível é obrigatória a instalação de um agente no dispositivo remoto, por exemplo um agente SNMP. Assim a auto-descoberta acaba por possibilitar apenas um conhecimento superficial da rede – a disponibilidade dos dispositivos na rede (se estão ligados ou desligados). Porém esta ferramenta goza de uma maior flexibilidade do que as restantes, dado que suporta variados tipos de comunicação para garantir a monitorização como o SNMP, o SSH, o WMI e até suporta os agentes utilizados pelo Nagios, o NSClient++ e o NRPE.

A interface Web do Zenoss, embora apresente muitas funcionalidades, acaba por ter um nível de complexidade algo elevado, revelando ter uma curva de aprendizagem de relevo, bem maior do que aquelas de outras ferramentas como o Nagios, e requerendo a utilização de alguns tutoriais para se conseguir aproveitar todo o potencial do programa.

Destaque porém para a excelente organização da interface, composta por um *dashboard* dividido por vários *portlets* com posições personalizáveis. Desses *portlets*, faz-se referência à utilização do Google Maps, permitindo dotar esta solução de um maior detalhe na localização dos dispositivos, detalhe este que não existe nos seus mais directos concorrentes, como o Cacti e o Nagios.

O envio de alertas é mais completo do que no Nagios, dado que permite enviar alertas para um grupo de utilizadores, oferecendo ainda a capacidade de definir uma hierarquia de alertas que possibilita garantir que os eventos serão definitivamente reconhecidos no final, mesmo quando não o são pelo primeiro utilizador com funções para tal.

Globalmente o Zenoss apresenta-se como uma solução de monitorização de redes muito completa, porém algo complexa, requerendo um tempo de aprendizagem bastante superior.

2.4 Comparação dos resultados das ferramentas

Neste subcapítulo são comparados os resultados obtidos com as três ferramentas de monitorização de redes analisadas, o Nagios, o Cacti e o Zenoss. Esses resultados são discutidos levando em conta a dificuldade de instalação e configuração, a apresentação e a dificuldade na utilização da ferramenta pelos utilizadores, as características de monitorização que cada ferramenta oferece, incluindo as funcionalidades de análise e criação de gráficos de desempenho, a forma como são realizadas as notificações dos problemas na rede, o suporte à ferramenta oferecido tanto pela empresa como pela comunidade, entre outros. Depois da análise comparativa justifica-se qual a melhor ferramenta a utilizar como motor de monitorização para a nova solução.

	Instalação	Configuração	Tratamento de Dados	Apresentação de Dados	Funcionalidades	Resolução de Problemas	Extensões e Comunidade
Cacti	+	++	++	+	-	-	-
Nagios	++	-	+	-	++	++	++
Zenoss	-	+	++	-	+	+	+

Figura 2.6 – Comparação de ferramentas

2.4.1. Instalação e configuração

A instalação de uma ferramenta de monitorização pode ser um processo complexo, tendo em conta o número de dependências que geralmente é obrigatório instalar com a devida antecedência. Das três ferramentas analisadas, a instalação do Zenoss foi a que se revelou mais acessível, devido essencialmente à existência de uma imagem de máquina virtual, para ser executada em ambientes Windows, que inclui já todas as dependências instaladas e o próprio Zenoss, pronto a utilizar. Porém esta opção poderá revelar-se pouco fiável dado que para se executar a máquina virtual é condição obrigatória ter um servidor com elevados requisitos mínimos e, para além disso, com esta escolha só é possível monitorizar um número máximo reduzido de dispositivos numa rede. O Zenoss suporta também instalação noutros sistemas operativos, como o Linux, sendo porém um pouco mais complicado. O Cacti também suporta a instalação em ambientes Windows, não recorrendo a máquinas virtuais como o Zenoss, mas requer que se instalem e se configurem todas dependências necessárias, uma a uma, pelo que a carga de trabalho resultante instalação total da ferramenta é quase igual à instalação desta ferramenta em ambientes Linux. Quanto ao Nagios suporta principalmente a instalação em Linux, com excelente documentação disponível e que guia o utilizador passo-a-passo no processo, mas também possibilita que a ferramenta corra numa máquina virtual, porém neste caso a documentação de apoio é inexistente, dificultando a tarefa para quem escolha esta opção. Levando em conta que o utilizador pretende utilizar todas as funções da ferramenta que escolher e ter ainda a garantia que tudo é feito com alto desempenho da mesma, a potencial facilidade de instalação da imagem de máquina virtual do Zenoss acaba por não ser aconselhada, dadas as suas limitações. Assim e devido à excelente documentação disponível, o Nagios e o Cacti são as ferramentas mais fáceis de instalar.

O processo de instalação não está concluído a partir do momento em que a ferramenta está instalada. A juntar a este processo está a fase de instalação de agentes para garantir a função básica de uma ferramenta de monitorização, ou seja a própria monitorização. Neste campo o Zenoss parece ser o que se destaca pela sua capacidade de auto-descoberta de dispositivos, no entanto esta descoberta automática por parte da solução não é totalmente vantajosa, no sentido em que esta funcionalidade apenas permite verificar os estados dos dispositivos com recurso ao comando PING, ou seja se estão ligados ou desligados. Para uma verificação mais detalhada da rede, o Zenoss, tal como o Cacti e o Nagios, requerem a instalação de agentes nos dispositivos remotos que funcionem como intermediários, ou seja mais carga a somar ao processo de instalação. Nesta fase da instalação da ferramenta, todas as três ferramentas são portanto negativamente semelhantes, não se destacando nenhuma.

A seguir à instalação é necessário proceder à configuração da ferramenta de monitorização. Neste campo o Nagios foi o que apresentou o pior método, obrigando à edição manual dos ficheiros de configuração, recorrendo a editores de texto por exemplo, e ao reiniciar do programa para que sejam aplicadas as alterações efectuadas, caso contrário o programa não as detecta automaticamente. Porém esta desvantagem acaba por se revelar uma potencial vantagem para o desenvolvimento de novas soluções baseadas no Nagios, como se verá mais à frente. Como o Nagios foi das primeiras ferramentas a aparecer no mercado, as que lhe seguiram puderam aprender com os seus erros e acabaram por corrigiram esta falha. Neste caso particular, dado que o Cacti e o Zenoss são posteriores ao Nagios, já oferecem na sua interface a opção de configuração da rede, facilitando por isso este processo.

2.4.2. Arquitecturas

As três ferramentas analisadas partilham algumas características no que diz respeito às suas arquitecturas. O nível mais baixo da arquitectura é o nível da monitorização ou a forma como é feita a recolha de dados dos dispositivos. O Nagios utiliza *plug-ins* que comunicam com aplicações agentes que são instaladas, nos dispositivos remotos, pelo utilizador. O Zenoss publicita a funcionalidade da auto-descoberta, mas o facto é que para um maior detalhe dos dados recolhidos é necessária a instalação de agentes SNMP nas máquinas remotas. Quanto ao Cacti com a utilização do seu *poller* que faz a verificação recorrendo também ao SNMP, requer igualmente instalação de agentes. Como a carga de configuração inicial associada a cada verificação é praticamente igual entre as diferentes ferramentas, o Nagios é aquela que se destaca, muito pela variedade de *plug-ins* disponíveis, possibilitando que se monitorize todos os tipos de dispositivos, e mesmo não existindo o *plugin* necessário ou desejado, é possível ao utilizador desenvolvê-lo.

O armazenamento dos dados é a segunda fase de operação de uma ferramenta de monitorização e neste caso é o Zenoss e o Cacti que se destacam com a utilização do RRDTool para guardar os dados de desempenho. A versão básica do Nagios (sem nenhuma extensão adicionada), como funciona essencialmente no campo da monitorização e resolução de problemas, mantém a sua informação guardada em ficheiros de configuração. Tendo o RRDTool características que possibilitam que as bases de dados não atinjam dimensões muito

grandes a partir de um certo limite, e dadas as suas características a nível da criação dados, representa a melhor escolha para guardar os dados recolhidos.

A apresentação dos dados é melhor na ferramenta Cacti. Embora o Zenoss também utilize o motor RRDTool para criação de gráficos, o facto é que o Cacti é essencialmente uma ferramenta de criação de gráficos, aproveitando o potencial do motor referido, e oferecendo mais funcionalidades para criar e visualizar representações gráficas do desempenho dos dispositivos, serviços e recursos da rede. O Nagios é muito pobre na secção dos gráficos, e embora permita criar e ver gráficos de disponibilidade e de desempenho, algo fracos na realidade, é acima de tudo uma ferramenta de monitorização e resolução de problemas, não tanto de análise.

No nível superior destas arquitecturas está a representação gráfica da ferramenta que em todas elas é dada por uma interface Web.

2.4.3. Apresentação e utilização

A apresentação de uma ferramenta de monitorização é um dos aspectos mais importantes a ter em conta. Uma ferramenta pode ter muito potencial, oferecer muitas funcionalidades, mas se a sua apresentação for fraca, confusa ou complexa então não será possível ao utilizador aproveitá-la no seu todo. Dado que o Nagios já existe há mais tempo que as outras duas ferramentas, seria de esperar que as sucessivas versões que têm vindo a ser lançadas, especialmente a última (a analisada foi a 3.0), fossem melhorando o aspecto da interface Web. A verdade é que, desde a sua primeira versão, as alterações na apresentação não foram assim tantas para serem notadas. O Nagios apresenta a pior apresentação das ferramentas analisadas, com um ar ultrapassado, embora organizada num compreensivo menu. Esta falha pode ser corrigida se o utilizador optar por instalar um dos vários *frontends* desenvolvidos pela comunidade, embora essas extensões não venham incluídas na versão base da ferramenta. A apresentação mais vanguardista é a do Zenoss, com uma interface Web desenvolvida em Ajax valorizada pela capacidade de personalização da área útil da informação, com recurso aos *portlets*. O Cacti oferece também uma boa organização a nível de apresentação. A nível de utilização a ferramenta mais compreensiva acaba por ser o Cacti, pois cada secção é acompanhada por blocos de informação que acompanham o utilizador e ajudam a perceber o que se pretende com as funcionalidades disponíveis. No que diz respeito às restantes ferramentas, tanto o Nagios como o Zenoss não possuem este tipo de cuidado, sendo que este último pode, numa fase inicial, revelar um nível de complexidade que poderá afastar potenciais utilizadores.

A juntar à apresentação é desejável que uma ferramenta de monitorização exiba um bom desempenho. Ao analisar a base de desenvolvimento das interfaces Web das ferramentas analisadas, verifica-se que a do Nagios é executada com base em CGIs escritas em C, podendo tornar-se potencialmente lenta em redes com um número elevado de dispositivos e serviços, ao contrário da interface do Nagios que foi desenvolvida em Ajax e por essa razão tem um melhor desempenho [12].

2.4.4. Funcionalidades

Uma ferramenta de monitorização é composta por várias funcionalidades para além daquelas associadas à monitorização. As funcionalidades básicas devem ser a visualização da informação da rede, a representação gráfica do estado e do desempenho da rede, e a geração de alertas. Mesmo garantindo estas funcionalidades, há ferramentas que disponibilizam ainda outras opções, algumas delas de grande interesse. De seguida comparar-se-ão as funcionalidades das três ferramentas.

2.4.4.1. Visualização da informação e representação gráfica

A visualização da informação da rede é feita através das interfaces Web das ferramentas e as três ferramentas apresentam os dados de maneiras diferentes. Das três ferramentas, o Cacti é aquela que se baseia praticamente numa forma de representação de dados - os gráficos de estado e desempenho. Mesmo só se concentrando numa única área apresenta-se como a ferramenta ideal para representação de dados, com as excelentes opções de personalização, com a adição de modelos de gráficos para diminuir o tempo de criação de novos gráficos, com a maior organização oferecida pelas árvores de gráficos, entre outros. O Nagios, por sua vez, tem uma compreensiva organização da apresentação de dados, com a vantagem de permitir ver ao detalhe todas as informações sobre os dispositivos e serviços, com a possibilidade de se criarem relatórios de disponibilidade, e de ver o estado geral da rede num mapa da rede, que no entanto revela ser tanto mais complexo quanto maior o número de dispositivos. A criação de gráficos no Nagios está reduzida a uma pobre secção de gráficos de disponibilidade ou desempenho, mostrando ser a ferramenta mais fraca nesta área. O Zenoss é das três ferramentas a que conjuga mais opções de visualização de informação, utilizando o Google Maps para visualização das localizações das várias redes numa cidade ou em países diferentes, uma característica de organização e apresentação ideal para empresas com escritórios espalhados por pontos geográficos distantes, disponibilizando a informação detalhada sobre os componentes da rede, no habitual formato de tabelas organizadas, e ainda oferecendo gráficos de desempenho personalizáveis que podem ser visualizados das mais diversas formas, como individualmente, em conjunto com outros, entre outras, sendo por isso a melhor e mais completa ferramenta nesta área.

2.4.4.2. Utilização de modelos

Os modelos são a forma que as ferramentas têm de simplificar alguns processos, como por exemplo a inserção de novas máquinas e de serviços, e a criação de gráficos. Sendo uma ferramenta essencialmente gráfica, o Cacti só oferece os modelos de gráficos, no caso do Nagios só existem os modelos de objectos, compostos pelos modelos de dispositivos, de serviços e de contactos, que são bem mais úteis pois permitem ajudar na definição de grupos de dispositivos, serviços e contactos que partilhem as mesmas características, estabelecendo uma base comum, imprescindível para acelerar o processo de configuração de redes compostas por muitos dispositivos [Ver Anexo A]. No Zenoss não existe só um tipo de

modelos, juntando aos tipos de modelos das duas anteriores ferramentas, as classes e os modelos de desempenho, pelo que a nível de facilidade de configuração de uma rede grande, o Zenoss torna-se a ferramenta ideal.

2.4.4.3. Resolução de problemas

Quando há alterações de estado da rede, poderá, por exemplo, significar o surgimento de problemas ou que se atingiu um estado crítico. Qualquer que seja o acontecimento, as ferramentas disponibilizam dois métodos para lidar com eles – resolução ou notificação. Duas das três ferramentas analisadas têm métodos igualmente muito bons. Tanto no Nagios como no Zenoss é possível definir acções que vão tentar resolver, de uma forma proactiva, os problemas, antes que estes escalem e antes que algum contacto seja notificado. Se for preferencial o uso de notificações, no Nagios é possível enviá-las para vários contactos de um mesmo grupo e configurar filtros para definir quando e como as enviar. No Zenoss são utilizados alertas com a opção de definir as hierarquias de alertas, uma função interessante e que garante que o problema será sempre reconhecido pelos responsáveis, e ainda a definição de regras para descrever como enviar os alertas. Em relação aos meios utilizados para envio das notificações ou alertas, o Zenoss está reduzido aos envios de alertas por correio electrónico ou para *pager*. O Nagios oferece uma variedade maior, possibilitando enviar notificações por correio electrónico, para pager, para telemóvel por SMS, para os programas de *instant messenger*, entre outros. De referir ainda que a comunidade do Nagios oferece ainda mais hipóteses de envio, necessitando que se instalem as devidas extensões para tal. O Cacti não possui qualquer mecanismo de notificações ou alertas. Assim, para notificar os contactos responsáveis pela gestão da rede sobre eventuais problemas na mesma, o Nagios é a ferramenta ideal.

2.4.5. Extensões e Comunidades

Tanto o Nagios como o Zenoss têm comunidades compostas por utilizadores, curiosos e programadores que suportam a ferramenta e estendem as funcionalidades, com novos *add-ons*, novos *plug-ins*, novos *frontends*, entre outros. O Cacti não possui qualquer comunidade digna de registo e quaisquer extensões conhecidas. Das duas ferramentas com comunidade extensa, o Nagios, tendo em conta que já existe há bastante mais tempo que o Zenoss, é aquela que tem mais conteúdo desenvolvido pela própria comunidade, que permite aumentar o potencial do Nagios, principalmente nas áreas onde falha em relação aos outros, como na área da interface gráfica e da representação gráfica dos dados de desempenho, permitindo assim torná-lo mais competitivo e atractivo. Contudo, seria desejável que o pacote da versão base do Nagios aproveitasse algumas destas extensões e já as trouxesse instaladas de origem.

A nível de suporte, o Zenoss oferece alguma documentação de apoio, embora seja um facto que a empresa disponibiliza as melhores opções de suporte apenas para as licenças comerciais. O Nagios por sua vez, muito por causa da sua comunidade, tem um excelente suporte, apoiado por uma excelente documentação de ajuda, tudo disponível de forma gratuita.

2.4.6. Resultados

Das três ferramentas estudadas, apenas duas representam ferramentas de monitorização mais completas, o Nagios e o Zenoss. O Cacti acaba por basear muitas das suas funcionalidades na representação gráfica do desempenho global da rede e individual dos dispositivos que a compõem. Como tal, é mais uma solução para utilizar como complemento do que como ferramenta de monitorização independente, tal como as duas primeiras. Na comparação das versões base do Nagios e do Zenoss, este último ganha clara vantagem com uma interface e apresentação superiores, com a característica de auto-descoberta que permite ter uma noção superficial da rede sem instalar qualquer agente, com as melhores representações do desempenho da rede, só ultrapassadas pelas representações do Cacti, entre outros, mas muitas vezes o Nagios é sobrevalorizado porque se analisa apenas a sua versão base. Levando em conta a extensa comunidade que esta ferramenta tem, existem milhares de *add-ons* e *plug-ins* que aumentam as suas capacidades e a tornam tão ou mais competitiva que as outras ferramentas. De referir que o Nagios é também, muitas vezes, usado com o Cacti para formar a equipa perfeita - monitorização, representação de dados e resolução de problemas.

2.5 O Nagios como motor de monitorização

As excelentes funcionalidades oferecidas pelo Nagios, o facto de toda a sua estrutura assentar sob ficheiros de configuração facilmente acessíveis pelos utilizadores e ainda a existência de uma forte comunidade que suporta o desenvolvimento de novas extensões, faz do Nagios uma escolha de eleição para núcleo central no desenvolvimento de novas interfaces Web que oferecem novas funcionalidades e tornam a ferramenta mais completa. De seguida faz-se a apresentação e a análise das mais importantes soluções desenvolvidas com base na utilização do Nagios como núcleo de monitorização.

2.5.1. Nconf

Lançada em Março de 2009, o Nconf é um *frontend* para o Nagios, desenvolvido em PHP e Perl, utilizando MySQL, com o objectivo de tornar o Web-GUI da ferramenta mais *user-friendly*, dotando-o com algumas funcionalidades que lhe faltavam, de forma a torná-lo também numa solução mais completa.

2.5.1.1. Visão Global

Esta solução é principalmente uma solução de configuração para o Nagios, permitindo abreviar esse mesmo processo, ou seja alterar todos os ficheiros de configuração dessa ferramenta, tanto os ficheiros globais como os ficheiros específicos das máquinas, de uma forma mais fácil e rápida, tarefa que se revela bastante complicada e morosa de realizar directamente no Nagios, que requer a alteração manual dos mesmos ficheiros.

O Nconf só funciona em ambiente Linux, sendo que os requisitos de instalação do mesmo são a instalação prévia do seguinte *software*:

- Servidor Web Apache;

- PHP;

- MySQL (com suporte a InnoDB);

- Nagios;

- Perl.

2.5.1.2. Funcionalidades

As funções principais do Nconf são na área da configuração do Nagios. Para além de permitir as alterações e adições de novos dispositivos, existe a opção de gerar a configuração do Nagios automaticamente. Este processo consiste na exportação dos dados da base de dados do Nconf, já com a nova configuração compatível, para o formato de configuração aceite pelo Nagios - os ficheiros de texto. Esta solução permite ainda que se analisem as alterações efectuadas nesses ficheiros de configuração, realizando um teste de sintaxe, antes que sejam gerados os ficheiros de configuração de saída. Esta é uma mais-valia na ferramenta, já que assim se evita gerar ficheiros de configuração com erros que possam comprometer toda uma instalação do Nagios.

Monitorização distribuída

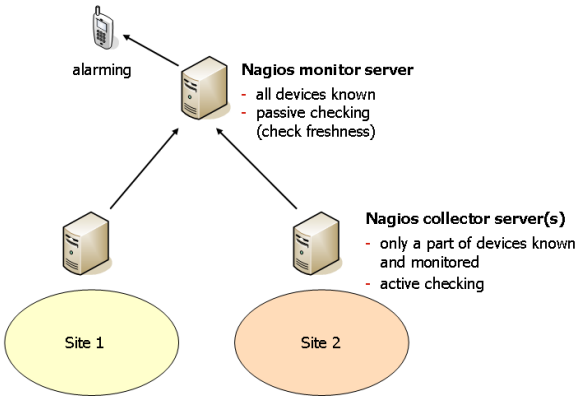

Figura 2.7 – Arquitectura da monitorização distribuída suportada pelo NConf

A configuração do tipo de monitorização distribuída é outra das funcionalidades que esta solução oferece. Uma só instalação do Nagios tem um limite no número de dispositivos ou serviços que pode monitorizar, pelo que utilizando alguns *plug-ins* é possível implementar um tipo de estrutura que suporta a monitorização distribuída. Essa estrutura apresenta uma composição bastante diferente da arquitectura centralizada, sendo composta por dois tipos de dispositivos:

- O servidor de monitorização;

- Os servidores de recolha.

Os servidores de recolha fazem verificações remotas em diferentes ambientes e passam-nas posteriormente ao servidor de monitorização que se responsabiliza pelo tratamento e apresentação dos dados recolhidos numa interface Web. Passam assim a existir dois tipos de verificações diferentes, as activas e as passivas. As verificações passivas são feitas pelo servidor de monitorização, quando este espera pela informação dos servidores de recolha. As verificações activas são realizadas quando estes últimos recolhem a informação remota e a encaminham para o servidor principal. Assim os servidores de recolha conseguem diminuir a carga de monitorização do servidor principal, distribuindo-a entre todos eles. Com o Nconf é possível criar novas entradas para servidores de monitorização do Nagios ou para servidores de recolha, ou visualizar a informação sobre servidores existentes. A versão básica do Nagios não possibilita a implementação deste tipo de arquitectura.

Importação de ficheiros CSV

Outra das características interessantes do Nconf é a possibilidade de importar ficheiros do tipo CSV (*comma-separated values*), com informação sobre novos dispositivos, serviços ou contactos que se pretendam adicionar à instalação do Nagios. O ficheiro CSV será processado e os objectos serão adicionados ao Nconf.

Existem duas formas de fazer esta importação, de uma forma personalizada, com a estrutura do ficheiro definida pelo utilizador, ou de uma forma pré-definida.

A importação com estrutura definida pelo utilizador tem como única restrição que o ficheiro contenha todos os atributos obrigatórios para o tipo de objecto que está a definir. Este tipo de importação possibilita adicionar qualquer tipo de objecto ao Nconf. O problema com esta forma de importação é que é necessário posteriormente alterar o *script* de importação, para informar a solução sobre o modo como deve fazer o mapeamento da informação, por coluna, que chegou no ficheiro, aos atributos que existem no Nconf.

A importação com estrutura pré-definida só permite que se adicionem dispositivos ou serviços mas, dado que obriga que os ficheiros CSV tenham uma estrutura específica, torna o processo mais fácil, não obrigando que se edite o script. A estrutura pré-definida decreta que as dez primeiras colunas são reservadas a atributos de dispositivos e que as seguintes cinco são reservadas a atributos de serviços, podendo ser repetidas as vezes que se pretender.

Em ambos os casos, a importação tem que ser realizada através da linha de comandos do Linux. Embora fosse preferível que esta função estivesse disponível a partir da interface Web, o facto é que existe suficiente documentação que acompanha o utilizador no processo.

Permissões

As permissões desempenham um importante papel no acesso à informação, com diferentes acessos para utilizadores distintos. Para um utilizador comum apenas estão disponíveis as

funções básicas. Para um administrador, a capacidade é aumentada, passando a estar também disponíveis as funções avançadas.

As funções básicas permitem ver ou adicionar:

- Máquinas;
- Grupos de máquinas;
- Grupos de serviços.

Também é possível usufruir do conceito de dependências das máquinas e visualizar, através de uma representação em formato de árvore, as informações do dispositivo e dos serviços que lhe estão associados. Existe igualmente um histórico que permite saber quando, por quem e que acções foram realizadas na interface.

Um utilizador normal pode ainda gerar uma configuração de Nagios.

As funções avançadas permitem configurar um maior número de características do Nagios, com opção de visualização ou de inserção dos seguintes componentes:

- Contactos;
- Grupos de contactos;
- Comandos de verificação e outros;
- Serviços;
- Períodos temporais;
- Classes de dispositivos;
- Modelos de dispositivos e serviços.

O administrador pode ainda visualizar ou criar novas entradas para servidores do Nagios, ou seja as máquinas que vão monitorizar a rede, e ainda para os servidores responsáveis pela recolha da informação remota.

É também possível alterar a configuração dos ficheiros estáticos do Nagios, como por exemplo o ficheiro principal de configuração *nagios.cfg*, da mesma forma como é feito no próprio Nagios, ou seja de uma forma mais primária - alteração dos ficheiros em editor de texto.

A interface Web é ainda personalizável ao gosto do utilizador. É possível alterar as características dos atributos e classes da aplicação, como por exemplo a sua visibilidade nos menus e que tipos de utilizadores os podem ver.

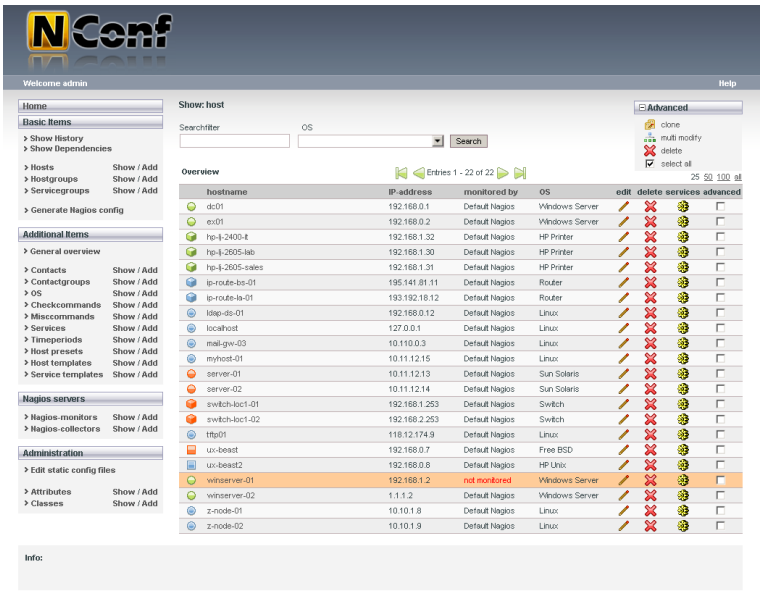

Figura 2.8 – Aspecto da interface Web do NConf

A nível de acessos, existem vários níveis de autorização que correspondem à permissão de acesso a parte ou a todas as características da ferramenta.

No Nconf existe uma preocupação em garantir uma rápida fase de configuração. Para tal existe uma funcionalidade interessante - a clonagem de serviços. Os serviços poderem ser clonados entre dispositivos, ou seja se existirem serviços comuns em duas máquinas, é possível copiar toda a configuração de uma para outra com um simples clique, poupando assim o tempo de inserção de um novo dispositivo e garantindo uniformidade na monitorização da rede.

2.5.1.3. Análise de Resultados

Um dos maiores e mais conhecidos problemas do Nagios é a sua morosa fase de configuração. Levando este facto em conta, o Nconf aparece como uma aplicação, totalmente gratuita, que permite reduzir em parte o tempo deste processo. Embora possibilite a criação de uma nova configuração de uma forma mais *user-friendly* através da interface Web, acaba por criar apenas um ficheiro compactado com todos os novos ficheiros de configuração e por não possibilitar a implementação automática do mesmo. Ou seja, o administrador da rede terá que ficar responsável pela execução da próxima fase, a instalação dos novos ficheiros de configuração na instalação do Nagios. Isto significa que a carga associada à aplicação das alterações no Nagios não é totalmente reduzida.

O facto de levar em conta o conceito de monitorização distribuída, permitindo criar novos servidores de monitorização e de recolha, torna o Nconf uma solução ideal para configuração do Nagios no cenário das grandes redes de monitorização. A possibilidade de definir novos objectos na instalação do Nagios, importando as definições a partir de ficheiros CSV, é outra

das características interessantes da solução, que poderá igualmente ser importante para aligeirar esse processo em grandes redes.

A grande falha do Nconf é a ausência da representação, tanto em tabelas como em gráficos, dos estados dos dispositivos na rede e do desempenho dos mesmos e dos seus recursos. Esta ferramenta acaba por ser apenas uma ferramenta de configuração do Nagios. Torna-se portanto indispensável aceder à interface Web do próprio Nagios para poder ver o estado e toda a informação relativa à rede. Seria de esperar que uma nova solução *frontend* para o Nagios tivesse mais capacidades para além de permitir configurar a informação do próprio, ou que pelo menos possibilitasse a integração com a interface existente.

O Nconf acaba por ser uma ferramenta de configuração completa para o Nagios mas falha ao não oferecer uma integração total com o mesmo. Já que funciona apenas no campo da configuração, seria desejável que pelo menos as duas interfaces Web fossem integradas para que se pudesse usufruir da soma da soma das suas funcionalidades, de uma forma mais fácil.

2.5.2. Centreon

Criado em 2007, o Centreon é um dos *frontends* do Nagios mais completo no mercado e é mais do que uma simples ferramenta de configuração do Nagios, cobrindo todas as funções oferecidas por esta ferramenta de monitorização e oferecendo uma grande diversidade de novos conceitos.

Para além de possibilitar uma configuração mais fácil do sistema, permite visualizar o estado da rede a partir da informação recolhida, criar e visualizar gráficos e relatórios, administrar o sistema, entre outras.

2.5.2.1. Visão Global

A arquitectura do Centreon está desenhada para permitir um modelo de monitorização distribuída, utilizando para tal o *add-on* NDOUtils, que permite exportar dados, recolhidos por vários servidores do Nagios, para uma base de dados MySQL. Em cada servidor do Nagios tem que se garantir apenas a instalação do Nagios e do NDOUtils, sendo que cada um ficará responsável pela monitorização de um determinado número de máquinas. A comunicação entre os servidores remotos e o Centreon é realizada quando o módulo *NdoMod*, existente em cada servidor, envia informação para um módulo *Ndo2DB*, existente no servidor do Centreon. Esse módulo realiza depois variadas operações para guardar na base de dados MySQL a informação recebida. Assim garante-se que toda a informação, vinda de diversos e diferentes pontos converge para o mesmo servidor central. Abaixo é possível ver uma ilustração deste processo.

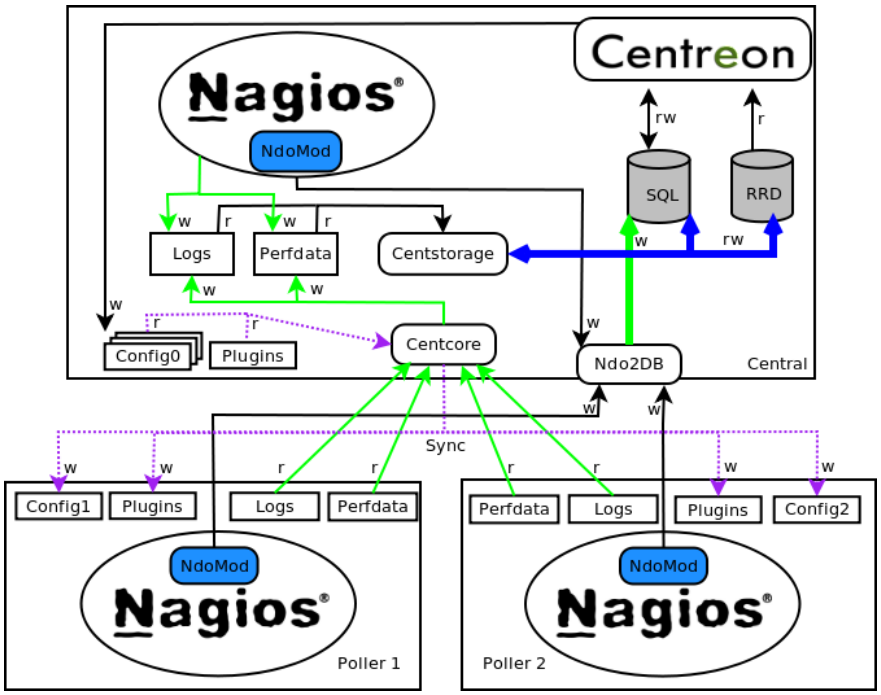

Figura 2.9 – Arquitectura do Centreon

Para a representação gráfica, o Centreon utiliza como motor a ferramenta RRDTool, que recebe os dados de desempenho dos vários servidores e a partir deles permite criar vários tipos de gráficos.

A instalação do Centreon poderá ser um pouco morosa, já que antes de se instalar a ferramenta de monitorização propriamente dita, é necessário garantir a instalação do seguinte software:

- Nagios;
- Plug-ins do Nagios;
- NDOUtils;
- Servidor Web Apache;
- MySQL;
- PHP;
- Biblioteca GD;
- RRDTool;
- Net-SNMP;
- Perl.

2.5.2.2. Funcionalidades

A interface Web desta solução divide-se em cinco secções, a de monitorização, a de visualização, a dos relatórios, a de configuração e a de administração do próprio Centreon.

Na secção de monitorização é possível ver o estado da rede, em grande detalhe, por dispositivo, grupos de dispositivo, grupos de serviços, *syslog*, *logs* de eventos, entre outros.

A secção de visualização possibilita criar e visualizar gráficos personalizados para diferentes áreas, os grupos de dispositivos e os grupos de serviços. A personalização existente permite definir um período de tempo durante o qual é apresentada a variação dos estados de determinado recurso, mostrando quatro gráficos do desempenho diário, semanal, mensal e anual.

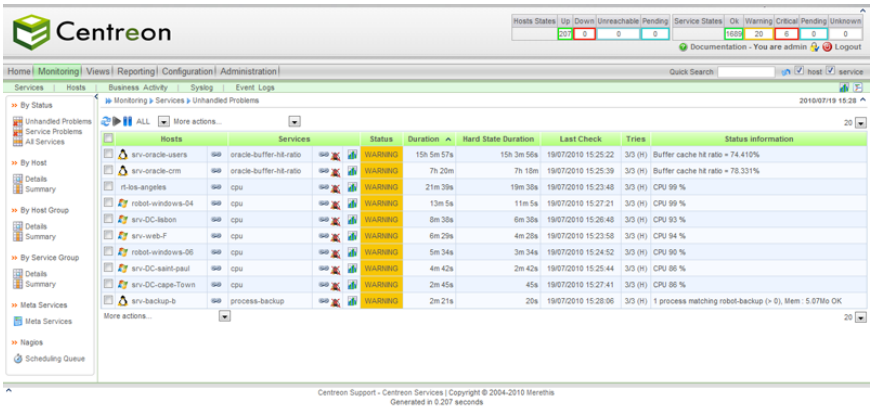

Figura 2.10 – Aspecto da interface Web do Centreon

Para se obter uma informação mais pormenorizada da rede a nível dos estados das máquinas e dos serviços a elas associados, o Centreon dispõem de uma secção de relatórios composta por um *dashboard* bastante completo. Cada dispositivo pode estar num estado de cinco possíveis:

-OK;

-Aviso;

-Crítico;

- Desconhecido;

- Indeterminado.

Também é possível ver o mesmo tipo de informação para os grupos de dispositivos e para os grupos de serviços.

O Centreon acrescenta alguns novos conceitos à interface do Nagios, entre estes está a secção de *Business Intelligence* onde é possível descarregar diversos tipos de relatórios apresentados em ficheiros de formato *pdf*, como por exemplo relatórios de disponibilidade e desempenho das máquinas ou relatórios do estado dos recursos das mesmas.

A habitual secção de configuração marca também presença nesta solução e possibilita configurar tudo o que é configurável manualmente no Nagios através da edição dos ficheiros de configuração. Esta configuração possibilita, entre outros, alterar os dispositivos e os serviços a eles associados, as notificações e a informação referente aos utilizadores. É possível criar novos ficheiros de configuração e exportá-los mas, ao contrário do *frontend* Nconf, possibilita também um carregamento automático, desses novos ficheiros de configuração, directamente no Nagios, através de uma interface presente no próprio Centreon.

Se o utilizador desejar poderá ainda alterar a informação referente à própria arquitectura do Centreon. São possíveis personalizações em quase tudo, incluindo na informação referente ao servidor que executa a solução e nos módulos *ndo2db* e *ndomod* do NDOUtils, correspondentes à arquitectura distribuída.

A solução oferece ainda a possibilidade de configurar a interface ao gosto do utilizador, desde o nível estético como a nível da autenticação de utilizadores, entre outro tipo de opções disponíveis.

O acesso à interface do Centreon não é igual para todos os utilizadores. Existe uma lista de controlo de acessos a partir da qual é filtrada a informação que cada utilizador pode ver. O administrador é o único utilizador com acesso total à ferramenta, existindo ainda utilizadores de operações, com acesso apenas à visualização detalhada do estado da rede, utilizadores de bases de dados, que só vêem a informação referente às bases de dados, sendo estes apenas alguns exemplos da longa de lista de permissões que é possível definir.

À semelhança do Nagios, com os *plug-ins*, ou do Zenoss com os ZenPacks, o Centreon tem as suas extensões. Estas extensões são módulos que aumentam as capacidades da ferramenta e estão divididas em três tipos, aquelas desenvolvidas pela equipa de desenvolvimento do Centreon, as desenvolvidas pela comunidade e ainda as extensões comerciais.

2.5.2.3. Análises de Resultados

Depois de uma análise mais detalhada chega-se à conclusão que de facto esta solução apresenta qualidades muito acima dos seus mais directos concorrentes. Ao contrário de muitos dos *frontends* desenvolvidos para o Nagios, esta ferramenta é mais do que uma mera ferramenta de configuração. É fácil pensar no Centreon como uma ferramenta de monitorização independente, de tão completo que é.

Visualmente apresenta-se com uma estética bastante limpa e com uma organização satisfatória que supera o próprio Nagios. A área de *Business Intelligence* é outra das características mais interessantes do Centreon. O facto de ser possível descarregar relatórios, em formato *pdf*, com a informação sintetizada dos estados, da disponibilidade e do desempenho de cada um dos dispositivos da rede é uma mais-valia para os administradores.

No entanto esta ferramenta poderá ser um pouco complexa para quem não conhece o ambiente do Nagios, já que se baseia, em parte, na configuração utilizando os parâmetros

deste. Querendo cobrir todas as funções já disponibilizadas pelo Nagios, o Centreon acaba por atingir um nível de complexidade aparentemente elevada para quem tem o primeiro contacto com a ferramenta, que não a torna *user-friendly* de todo.

O facto de se basear numa ferramenta *open-source*, torna esta solução também *open-source* e gratuita. No entanto se um utilizador desejar aumentar as potencialidades da solução e utilizar as extensões disponíveis, mantendo-se no campo do *software* livre, só poderá usufruir das extensões *core* ou daquelas desenvolvidas pela comunidade. As extensões comerciais, desenvolvidas pela equipa de desenvolvimento do Centreon, são exclusivas a quem por elas pagar.

2.5.3. Opsview

Lançado em 2003, o OpsView é actualmente disponibilizado em duas versões, a versão gratuita Community e a versão paga Enterprise. Segundo a empresa, ambas as versões são completamente iguais a nível de funcionalidades, embora a versão da comunidade não tenha suporte, nem manutenção ou garantia, características presentes apenas na versão com licença paga.

2.5.3.1. Visão Global

A arquitectura do Opsview divide-se em três camadas distintas: a interface Web, o servidor da aplicação e as fontes de dados. A primeira camada é aquela que permite a comunicação entre o utilizador e a aplicação. A camada do servidor de aplicação é composta por uma instância do Catalyst, um *framework* de aplicações Web, que gere a aplicação Web, lidando com todas as páginas dinâmicas apresentadas. A última camada é composta pela instalação do Nagios e por três bases de dados MySQL, uma para guardar as configurações da própria aplicação, outra para guardar a informação relativa aos dispositivos monitorizados e outra para guardar os dados de desempenho destes e um histórico.

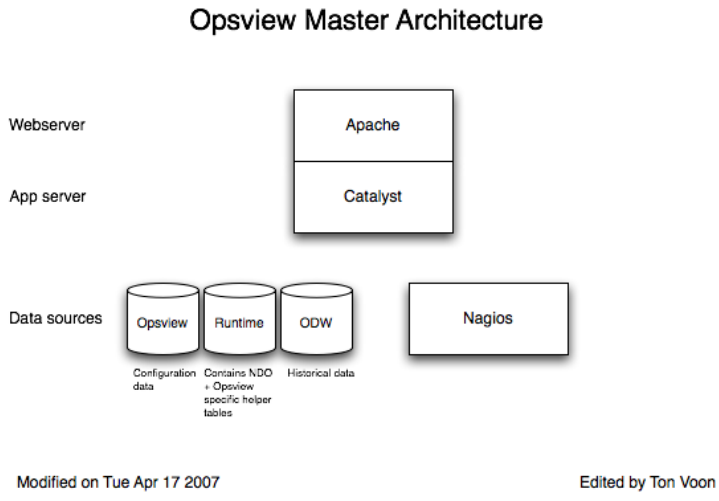

Figura 2.11 – Diagrama da arquitectura principal do Opsview

À semelhança do Centreon, também o Opsview suporta o conceito de arquitectura distribuída de monitorização para permitir ter vários servidores de monitorização activos, cada um com função de verificar diferentes dispositivos em diferentes locais. O conceito consiste em ter um servidor principal de monitorização e ter outros escravos que recolhem a informação, que será mais tarde lida pelo primeiro. A comunicação é realizada através de túneis SSH, e pode ser iniciada tanto pelo servidor principal como pelos secundários.

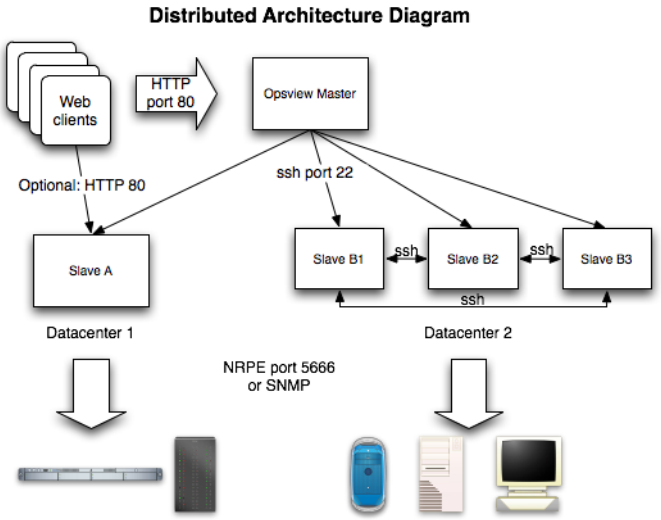

Figura 2.12 – Diagrama da arquitectura distribuída do Opsview

A instalação do Opsview testada foi a versão da comunidade (gratuita) que é executada numa máquina virtual, uma versão que já vem com todas as dependências instaladas, inclusive com uma instalação do Nagios, e que é executada na aplicação *vmware*. Tirando as possíveis complicações que podem surgir na fase de definição do IP estático a utilizar pelo *vmware* para que seja possível aceder à interface Web, todo o processo de instalação é bastante fácil e em pouco tempo o Opsview está a funcionar.

2.5.3.2. Funcionalidades

O Opsview suporta a função de auto-descoberta de capacidades SNMP, permitindo que dispositivos que suportam este protocolo sejam detectados e monitorizados facilmente.

A partir da interface Web do Opsview é possível configurar todo o sistema do Nagios, característica essencial em qualquer ferramenta que o utilize como motor de monitorização. A disposição das várias funções disponíveis é feita de uma forma bastante acessível e perceptível para o utilizador, estando esta solução dividida em várias secções.

A secção de estado permite analisar em detalhe o estado de cada dispositivo ou serviço registado no sistema, seja no formato de tabelas, em grupos e por hierarquias, ou num mapa da rede idêntico àquele que o Nagios possui na sua própria interface (que se pode revelar algo confuso se a rede for composta por várias dezenas de dispositivos, embora ofereça alguns métodos para reduzir a complexidade mas que acaba por complicar igualmente a leitura do

mapa), e analisar os eventos ocorridos, considerando que um evento é cada uma das acções realizadas na interface, como por exemplo a inserção de um novo dispositivo na rede. Na secção de alerta é possível ver todos os alertas disponíveis na rede, sejam avisos registados ou recursos em estado crítico, ou seja todos os problemas da rede.

O Opsview possibilita também a criação personalizada de mapas da rede. Para tal utiliza um *add-on* de visualização para o Nagios chamado NagVis que permite simular ambientes de infrastruturas de rede. A criação e visualização de gráficos, ao contrário da maior parte das ferramentas de monitorização, não é feita com recurso ao RRDTool. Para esta tarefa, a ferramenta usa o Flot, um programa de criação de gráficos baseados na linguagem de *scripts javascript*. Os gráficos oferecem uma série de características interessantes como a possibilidade de definir períodos para a apresentação dos mesmos e ainda efectuar *zoom* em qualquer parte do gráfico escolhido, para que se obtenha um maior detalhe. A personalização permite ainda que se defina o tipo de gráfico, as unidades e as séries a utilizar, entre outras opções.

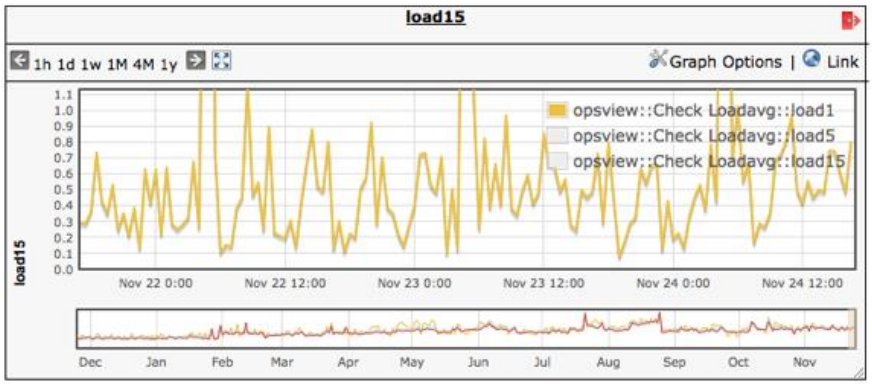

Figura 2.13 – Exemplo de gráfico de desempenho da carga do CPU do computador

Para além disso é possível configurar a utilização de SNMP para recolha de informação em cada dispositivo por parte do MRTG, uma ferramenta que permite criar gráficos com base na informação dos recursos que está a monitorizar.

A configuração do Nagios no Opsview não podia ser mais detalhada. Desde definir métodos de notificação e períodos de tempo, a alterar os comandos a utilizar nas verificações e criar ou alterar os contactos, é extensa a configuração que se pode realizar na ferramenta de monitorização que dá suporte ao Opsview. Qualquer alteração efectuada, respeitante ao servidor do Opsview ou à configuração do Nagios requer que o utilizador recarregue o sistema manualmente, carregando num botão disponível no topo da interface. Esta solução não realiza essa acção automaticamente.

2.5.3.3 - Análises de Resultados

O Opsview acabou por se revelar uma ferramenta de monitorização de qualidade, estendendo as capacidades do Nagios tanto a nível de monitorização como de configuração. Uma das

melhores características desta solução é o facto de integrar diversas aplicações, o NagVis, o Net-SNMP, o MRTG, o NDO e o Flot, que a tornam numa ferramenta mais completa que aquela que lhe serve de base.

A nível da instalação, sai privilegiado quem optar por instalar o Opsview numa máquina com sistema operativo Windows, já que a instalação é bastante fácil, bastando para tal instalar uma máquina virtual, que já traz as dependências instaladas, carregar a imagem do programa e fazer algumas configurações iniciais, desde que o utilizador possua um servidor com os requisitos mínimos, que são consideravelmente altos, para suportar o funcionamento da máquina virtual. Quem optar pela instalação em sistemas operativos Linux ou outros, terá uma carga superior de trabalho e tempo dispendido, já que é preciso instalar todas as dependências, uma a uma, antes de se instalar o Opsview.

Um ponto negativo no Opsview é a necessidade de se activar o recarregamento manual da configuração do Nagios, após a inserção de uma nova máquina ou serviço, sendo necessário para tal tarefa que o utilizador carregue num botão designado por "Configuration Status". Só depois disso é que as novas máquinas passam a ser monitorizadas ou as alterações efectuadas têm efeito. Mesmo assim para que seja possível ver a informação relativa ao dispositivo que se acabou de adicionar, é preciso garantir que se associa pelo menos um recurso ao mesmo. A ferramenta não permite visualizar na lista de dispositivos monitorizados, a informação de dispositivos adicionados que não tenham pelo menos um recurso associado.

Outra das desvantagens desta ferramenta é a impossibilidade de instalá-la sobre uma instalação de Nagios já existente, pois o Opsview depende de uma determinada versão do Nagios. Para quem já trabalha com o Nagios, torna-se um bastante desmotivador ter que desinstalar toda a instalação do mesmo para poder utilizar esta solução, quando provavelmente já está configurada com centenas de dispositivos.

Existe também uma diferença entre a versão da comunidade e a versão *enterprise* do Opsview. Embora ambas ofereçam as mesmas funcionalidades básicas, no que diz respeito aos módulos de extensões a realidade é diferente. A versão *enterprise* acaba por disponibilizar módulos exclusivos, entre eles a possibilidade de gerar relatórios sobre o estado da rede (*Business Intelligence*), de enviar mensagens *sms* de alerta e ainda de melhorar a gestão da rede com o RANCID.

2.6 – Outras ferramentas

Para além destas ferramentas *open-source* principais analisadas, existem muitas outras na área das ferramentas baseadas no Nagios, sendo que a maior parte delas figura como ferramenta de configuração deste. A seguir listam-se algumas outras importantes ferramentas.

- NagiosQL

- Lilac

- Nag2Web

- NagiosAdmin

- Nagios Configurator

Capítulo 3

Descrição do trabalho desenvolvido

O trabalho desenvolvido consiste numa solução Web integrada com a ferramenta de monitorização Nagios, que possibilita realizar a configuração de uma rede, a sua monitorização com a verificação do estado dos dispositivos, recursos e serviços que a compõem, emitir avisos quando surgem problemas e ainda ter acesso a uma análise mais detalhada de toda a rede, através da criação e visualização de diversos formatos de representação do seu desempenho ao longo do tempo. Para além de oferecer as principais características de uma ferramenta de monitorização, esta solução disponibiliza ainda algumas ferramentas que se pretende que sejam de apoio à gestão de uma rede. Esta solução dá pelo nome de Athena, inspirado na conhecida deusa da sabedoria da Grécia Antiga e, tal como ela, esta solução visa dar sabedoria, particularmente dotar os administradores de um melhor conhecimento de toda uma rede de dispositivos.

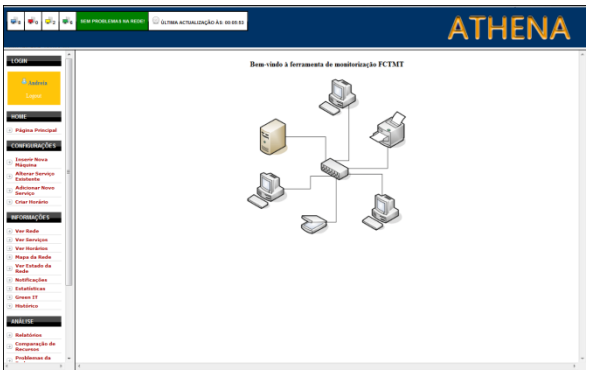

Figura 3.1 – Aspecto da interface Web do Athena

Os requisitos para executar a aplicação Athena são a instalação prévia do seguinte software:

- Servidor Web Apache;
- Base de dados MySQL;
- PHP;
- Nagios;
- Plug-ins do Nagios.

Esta nova solução foi desenvolvida com as linguagens de programação PHP, PHP XML, Javascript e CSS, e para as bases de dados foi utilizado o MySQL [Ver Anexo B]. A solução divide-se em três áreas principais: a área de configuração, a área da visualização do estado da rede e a área de análise de custos, e é apresentada através de uma interface Web acessível através de qualquer browser.

A área útil da interface Web é decomposta em três subáreas:

- Barra de informações gerais;

- Menu de opções;

- Área de visualização do conteúdo.

No topo da interface Web existe uma barra que mostra as informações gerais do sistema, o número total de dispositivos, os dispositivos ligados, os dispositivos desligados e os dispositivos com aviso, a hora da última actualização do sistema e ainda o número de problemas existentes na rede. Esta barra visa sintetizar a informação geral da rede.

3.1. Configuração da Rede

Um dos primeiros passos no desenvolvimento desta solução foi dado a partir de uma característica menos positiva do Nagios, a sua morosa configuração. O facto de ser obrigatória a edição manual de cada ficheiro de configuração cada vez que se pretende adicionar um novo dispositivo ou novo serviço para monitorizar, ou proceder a alterações nos dados existentes, é sem dúvida uma característica desencorajadora. De forma a colmatar esta falha, um dos primeiros objectivos no desenvolvimento desta nova solução foi tornar este processo muito mais *user-friendly*. Assim, através da interface Web do Athena é possível configurar o Nagios de forma imediata, com as seguintes opções:

- Inserção de um novo dispositivo para monitorização;

- Remoção de um serviço existente;

- Inserção de um novo serviço para monitorização;

- Criação de um horário de funcionamento e de não funcionamento.

3.1.1. Inserção de um novo dispositivo

Na secção de inserção de novos dispositivos é possível inserir três tipos de dispositivos: os dispositivos com sistema operativo Linux, os dispositivos com sistema operativo Windows e ainda *routers*. Este processo é realizado uma vez por cada dispositivo e consiste em três fases distintas:

1. Definição das características principais do dispositivo;

2. Escolha dos recursos para monitorizar;

3. Associação do dispositivo a uma sala.

A definição das características do novo dispositivo, que pode ser um computador, um servidor ou um *router*, requer a definição do nome de identificação a utilizar no sistema Athena, do IP ou do nome pelo qual é identificado na rede, da sua descrição, do número máximo de dias que

pode estar ausente da rede e de um modelo de horário com os períodos de funcionamento e de não funcionamento.

É também necessário definir a informação referente ao proprietário do dispositivo, ou seja o nome e o correio electrónico de contacto do mesmo. Nesta fase é possível que o utilizador escolha se pretende receber notificações sobre os eventos que acontecem na rede. Para cada novo dispositivo a inserir é criado um modelo de notificações diferente, personalizado pelo utilizador. Essa personalização consiste na definição do nome do modelo, na escolha horário para envio de notificações, no intervalo entre envios de notificações, e ainda nas opções a utilizar para o envio de notificações.

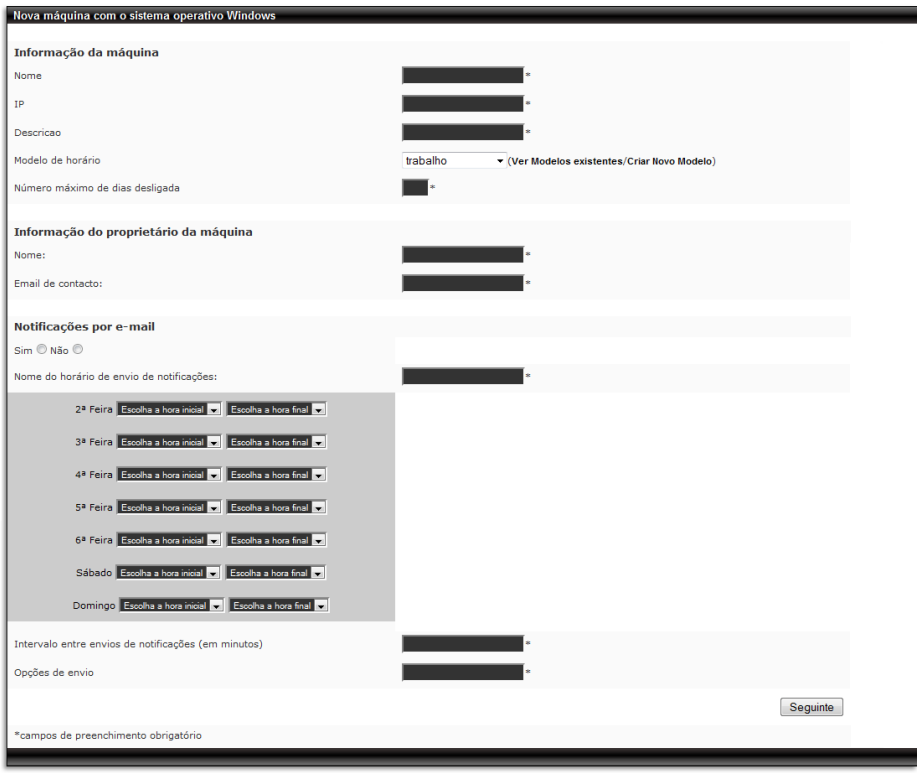

Figura 3.2 – Definição de um novo dispositivo

Depois de definidas as características do novo dispositivo é necessário escolher os recursos que se pretende monitorizar. As possibilidades de escolha são a carga do CPU, a memória virtual, a memória física, o espaço no disco rígido e o tempo que o dispositivo está ligado. Estes recursos aplicam-se apenas a computadores ou servidores com Windows ou Linux, dado que a Athena não possibilita monitorizar estes tipos de recursos em *routers*.

Figura 3.3 – Associação de serviços a um novo dispositivo

Uma vez definidos os serviços, e para concluir a inserção de um novo dispositivo na rede, é necessário associá-lo a uma sala. Esta associação pode ser realizada numa sala já existente ou, caso se pretenda, numa nova sala que deverá ser criada na secção Mapa da Rede. Terminado todo este processo, o Athena faz a implementação automática e imediata das alterações no Nagios, não sendo necessário que o utilizador execute manualmente esta tarefa, tal como algumas soluções baseadas nesta ferramenta exigem.

3.1.2. Alteração de serviço existente

Depois de se ter realizado a configuração de um novo dispositivo na rede, a informação é guardada e o dispositivo começa de imediato a ser monitorizado pelo Nagios. É possível ver os dados dos recursos escolhidos para serem verificados, mas é também possível, a qualquer momento, alterar os recursos que estão associados a qualquer dispositivo. Essa alteração consiste na remoção de um recurso que já não se pretenda monitorizar, sendo os efeitos da remoção igualmente imediatos no Nagios. Quando a remoção fôr concluída, a próxima verificação agendada já não levará em conta o recurso removido.

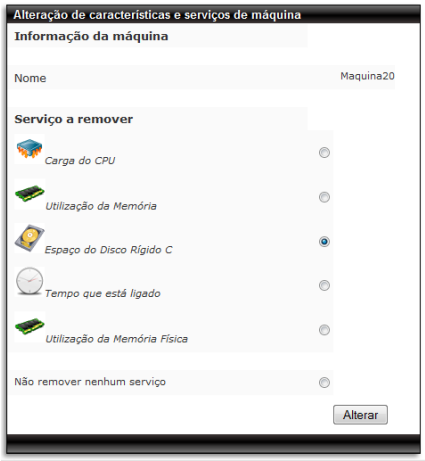

Figura 3.4 – Alteração dos serviços a verificar num dispositivo

3.1.3. Adicão de novo serviço

Também é possível fazer a adição de um novo serviço a um dispositivo existente, para monitorização. Essa escolha é feita de uma forma simples e bastante perceptível para o utilizador.

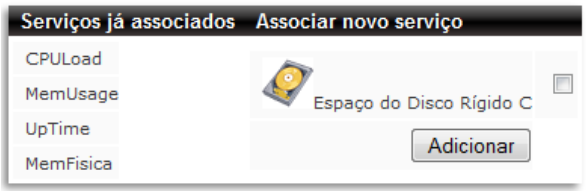

Figura 3.5 – Associação de uma nova verificação de um recurso a um dispositivo já existente

3.1.4 - Criação de um horário

O Nagios oferece o conceito de *timeperiods*, que consiste na possibilidade de definir quando são feitas as verificações e enviadas as notificações, e o Athena aproveita esse conceito quando se definem as notificações em novos dispositivos na rede. Mas para além disso oferece um outro conceito – os modelos de funcionamento e de não funcionamento dos dispositivos. Com esta nova característica é possível definir um intervalo temporal, limitado pela hora inicial e hora final, para as horas em que um dispositivo deve estar ligado e as horas em que dispositivo deve estar desligado. Este nova característica pretende ajudar na gestão da energia gasta por cada dispositivo, especialmente para evitar aquelas horas em que os dispositivos estão ligados a gastar, sem ninguém os estar a utilizar. Na criação de um novo modelo é necessário definir um intervalo por cada dia da semana.

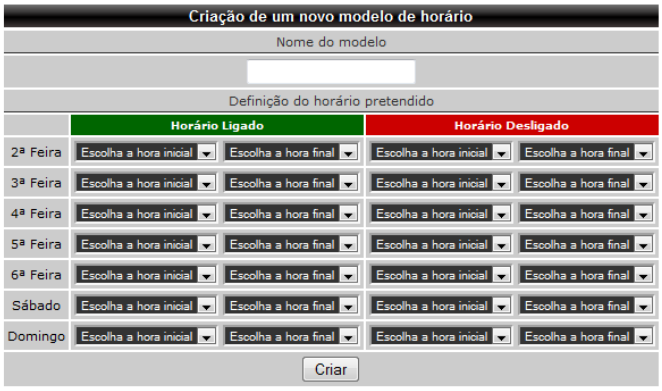

Figura 3.6 – Criação de um novo modelo de horários

Outro factor importante, que é estabelecido durante a inserção de um novo dispositivo na rede, é dado pelos números de dias que o mesmo pode estar ausente da rede. Esse factor conjugado com os modelos de horários citados permite ao utilizador evitar a criação de notificações resultantes de falsos problemas como consequência do desrespeito pelos horários definidos para um determinado dispositivo. No fundo cria-se um novo estado para os dispositivos elevando a três os estados possíveis dos dispositivos na rede: ligado, desligado ou ausente.

3.2. Informação da rede

Para além da configuração possibilitada pelo Athena, existe outra área, um pouco mais extensa: a área de visualização de informação da rede e de todos os seus componentes. Esta área é composta por oito subáreas:

- Visualização da rede;

- Visualização de serviços;

- Visualização de horários;

- Mapa da Rede;

- Visualização do estado da rede;

- Visualização dos modelos de notificações;

- Visualização das estatísticas da rede;

- Histórico.

3.2.1. Visualização da rede

A informação geral da composição da rede é visualizável a partir de uma listagem de todos os dispositivos presentes na rede, agrupados por tipo (dispositivos com Windows, dispositivos com Linux e *routers*). Para cada dispositivo é possível visualizar cinco características: o nome pelo qual é reconhecido no Athena, o IP ou nome na rede onde está a ser monitorizado, a sua localização no mapa da rede, o modelo de horário que está a utilizar e ainda o seu estado actual, resultante da última verificação efectuada.

Figura 3.7 – Secção de visualização da informação da rede

3.2.2. Visualização de recursos

Cada dispositivo tem recursos associados e nesta secção é possível ver a informação resultante de cada verificação a esses recursos. Essa informação pode ser vista no formato de relatório composto pela informação directa, devolvida pelo dispositivo ao Nagios, ou no formato gráfico. Para ser de fácil compreensão, esta secção adopta um modo de visualização simplificado que mostra apenas os serviços associados a um dispositivo de cada vez.

Figura 3.8 – Secção de visualização da informação dos serviços I

Foi criado ainda um sistema de quatro cores que possibilita entender melhor os estados dos serviços. Para percebê-lo é necessário compreender que no Nagios se definem níveis mínimos e críticos, para definir os estados dos dispositivos e dos serviços. Por exemplo analisando a carga do CPU de um computador, abaixo de 80% temos um estado normal, entre 80% e 90% o computador passa a um estado de aviso, acima de 90% passa a um estado crítico, ou seja surge um problema. Assim, existem quatro cores para identificar os estados: existe o verde que representa um estado OK do serviço, o amarelo que representa um estado de aviso do serviço, o laranja que representa um serviço crítico e um vermelho que representa um dispositivo desligado ou ausente da rede. Para dispositivos no estado vermelho, a representação gráfica dos serviços é desactivada.

Um relatório de informação é composto pelo nome do serviço, o nome do dispositivo a que este pertence, o estado em que se encontra e as datas da última e da próxima actualização do estado do serviço, como se pode ver no exemplo da figura seguinte.

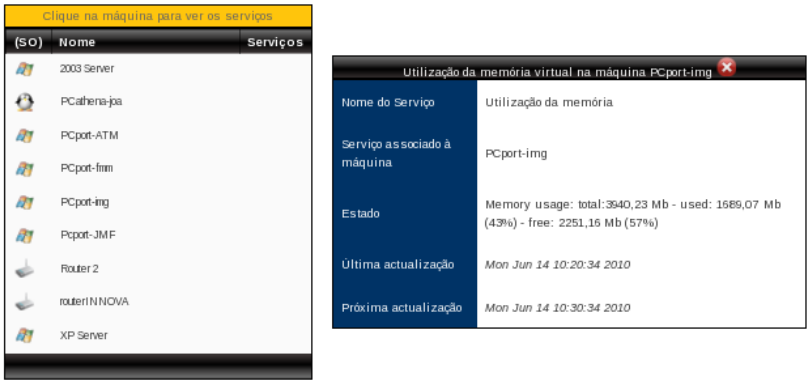

Figura 3.9 – Secção de visualização da informação dos serviços II

Outra forma de ver o estado do serviço, não tão detalhada mas mais simples é através da representação gráfica. Esta representação gráfica pode, no entanto, variar consoante o serviço em causa. O serviço carga do CPU é o único a utilizar um gráfico de barras para a representação dos seus valores de utilização. Para os restantes serviços optou-se por um

gráfico do tipo tarte (*pie*), por oferecer uma interpretação fácil dos dados dos serviços. Neste formato o estado de cada serviço é apresentado em percentagem. É possível ainda guardar os gráficos para posterior análise. Nas figuras seguintes estão representados dois exemplos deste formato.

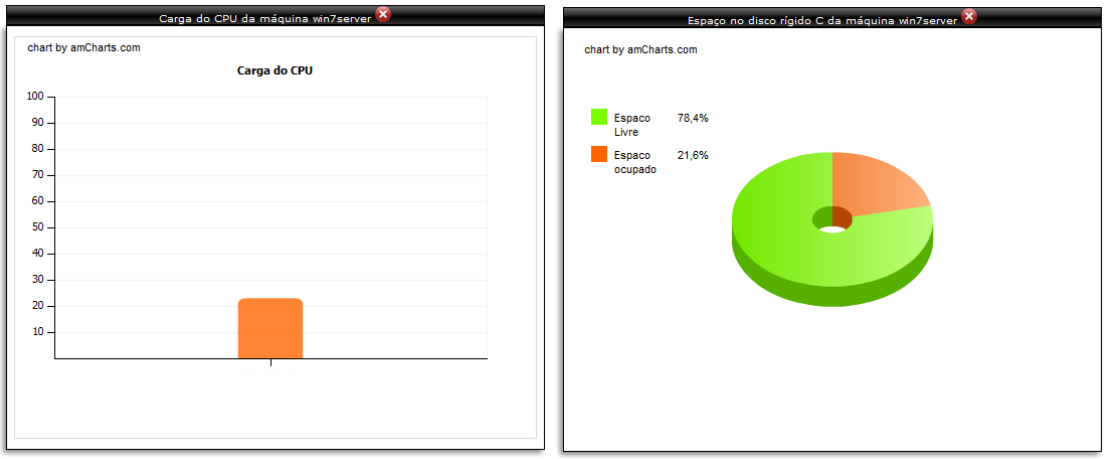

Figura 3.10 – Tipos de gráficos de serviços: a) Barras b) *Pie*

3.2.3. Visualização de horários

Depois de o utilizador definir um novo dispositivo e de o associar a um modelo de horário de funcionamento e não funcionamento, é possível visualizar e analisar as representações gráficas de todos os horários disponíveis na solução, para que se perceba se foi feita a melhor escolha. Estes modelos de horários têm ainda um papel de extrema importância na secção de análise de custos que se apresentará mais à frente.

3.2.4. Mapa da rede

O Athena dispõe de uma forma gráfica de representar a composição da rede. É possível criar salas à medida do utilizador, ou seja representações virtuais das disposições reais, implicando para tal a definição do seu nome e do seu tamanho.

Uma sala é criada sempre em formato de quadrado, com a definição da sua dimensão lateral N. Numa sala vazia existirão portanto N^2 posições disponíveis para localização dos dispositivos. Para inserir um dispositivo numa dada posição, basta clicar sobre a posição pretendida e escolher o dispositivo que se pretende a ela associar.

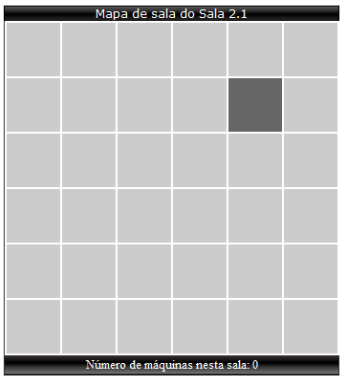

Figura 3.11 – Alocação de um dispositivo numa sala

Uma vez alocado, o dispositivo passa a pertencer a essa sala, sendo representado por um ícone de computador ou de *router*, com aspecto variável consoante o seu estado. A partir deste momento, clicar nesse ícone possibilita a visualização da informação individual actualizada desse dispositivo, bem como dos recursos que lhe estão associados.

Existe ainda a possibilidade de, a qualquer momento, remover um dispositivo de uma determinada sala e alocá-lo a outra sala.

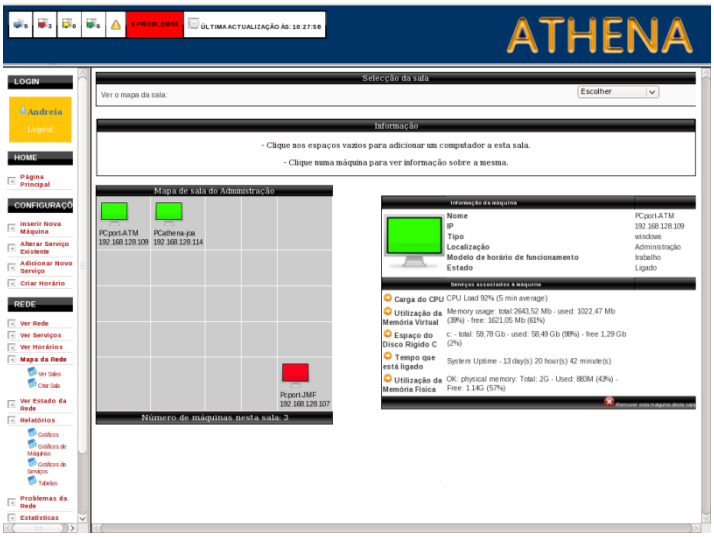

Figura 3.12 – Secção de mapa da rede

3.2.5. Visualização do estado geral da rede

Na secção do estado geral da rede é possível ver um conjunto de dados que permite ter a noção da composição e distribuição da rede. Existem gráficos estatísticos que mostram diferentes tipos de informação:

- A composição da rede por tipos de dispositivos;

- As máquinas por sistemas operativos;

- Os serviços por estados.

É também possível verificar qual o estado global da rede registado na última hora, para todos os dispositivos e todos os serviços registados, através de uma listagem com cada entrada distinguida pela hora de verificação.

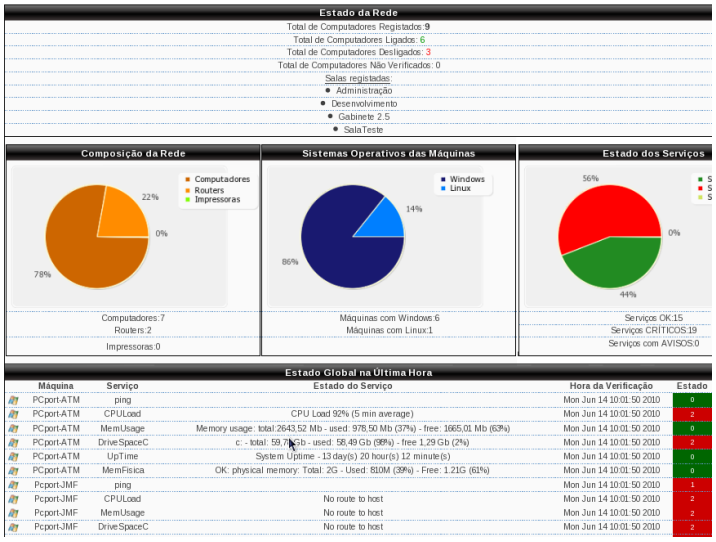

Figura 3.13 – Secção de estado geral da rede

3.3. Análise da Rede

Uma das secções mais completas da nova solução é a secção de análise da rede que permite que o utilizador examine o comportamento global e individual da rede, através de diversos tipos de análise. É possível criar e visualizar relatórios, comparar recursos, visualizar de uma forma detalhada os problemas na rede, analisar custos, identificar os dispositivos com sobre e subutilização, agendar acções e ainda estimar o estado real dos dispositivos com base nos valores dos seus recursos.

3.3.1. Relatórios

A observação dos estados dos dispositivos e serviços da rede pode ser feita através da visualização da informação por eles devolvida quando são verificados pelo Nagios. No entanto esta análise não permite estudar o seu comportamento ao longo do tempo. Para tal foi criada uma secção de relatórios, que permite ver o desempenho dos componentes da rede ao longo do tempo, em formato gráfico ou em tabelas. Em ambos os casos é possível acompanhar a evolução dos estados e perceber quais as suas tendências no tempo.

Os gráficos representam o comportamento de um só dispositivo ou de um só serviço de cada vez, ao longo do dia escolhido pelo utilizador. Os gráficos existentes são divididos em dois tipos de gráficos: os gráficos de disponibilidade, que informam se os dispositivos estão ligados ou desligados e os gráficos de estado, que informam sobre os estados dos recursos associados aos dispositivos. No exemplo abaixo é possível ver um gráfico de disponibilidade

de um computador, ao longo de um dia. Cada registo do estado é um valor resultante de uma média de valores recolhidos ao longo de cinco minutos.

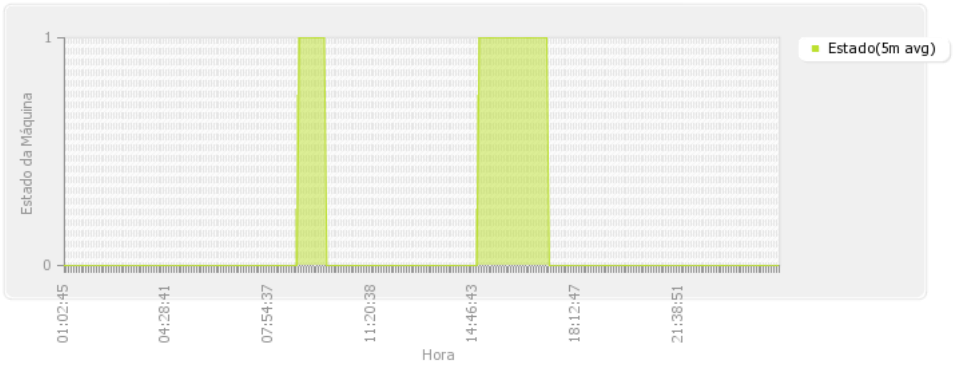

Figura 3.14 – Exemplo de gráfico de disponibilidade de um dispositivo

No caso de alguns serviços, a apresentação é composta por dois gráficos, geralmente um gráfico com a percentagem de serviço utilizado e outro com a percentagem de serviço livre. No exemplo abaixo tem-se o estado da memória física de uma determinada máquina no dia 22 de Julho de 2010.

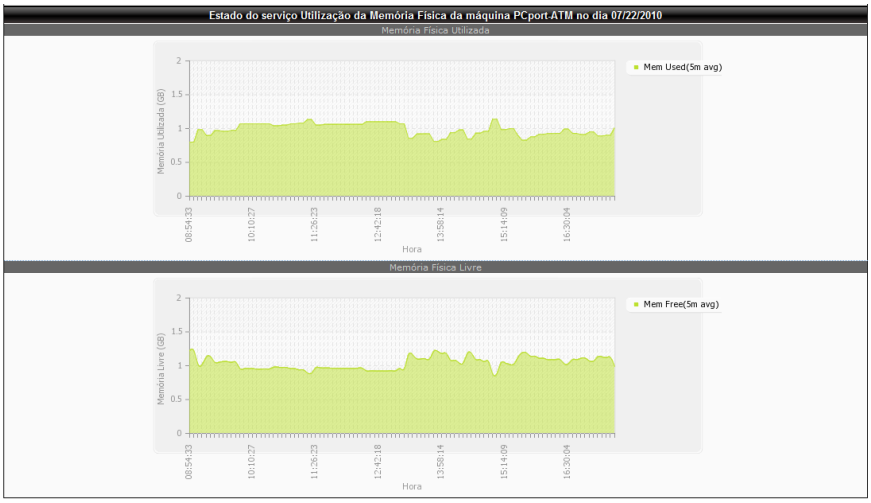

Figura 3.15 – Exemplo de gráfico de estado de um serviço de uma máquina

As tabelas, por sua vez, permitem ver os resultados individuais das verificações efectuadas ao longo de um dia de uma forma mais detalhada, mas de interpretação mais difícil.

3.3.2. Comparação de recursos da rede

A área de comparação de recursos da rede possibilita que o utilizador observe quais as três maiores percentagens de utilização dos recursos principais em dispositivos diferentes nesse mesmo instante. A acompanhar cada gráfico representativo das utilizações dos recursos, a solução disponibiliza algumas sugestões. Assim, é possível detectar quais os dispositivos que

estão perto de atingir um estado crítico, possibilitando que o administrador o antecipe. É ainda possível criar uma comparação personalizada, escolhendo as máquinas e um dos serviços que têm em comum.

Figura 3.16 – Exemplo de comparação instantânea dos principais recursos da rede

3.3.3. Visualização de problemas

No Athena a definição de um problema pode ser vasta, ou seja um problema pode ter várias origens. Se uma máquina estiver desligada fora do seu horário de funcionamento obrigatório, se uma máquina estiver ligada no seu horário de não funcionamento, se estiver ausente da rede mais do que o número de dias permitido, se um recurso estiver com excesso de utilização ou se estiver a devolver um resultado fora do normal, todas estas situações são consideradas potenciais problemas.

Para além do envio de notificações, esta solução reporta os problemas ao utilizador de duas outras formas distintas. A barra de informações gerais da rede, situada no topo da interface, sofre uma alteração visual quando surgem problemas, aparecendo um aviso com o número de problemas que existem nesse momento na rede. Clicando nesse aviso, o utilizador é levado à área de problemas onde poderá ver em detalhe a descrição dos problemas.

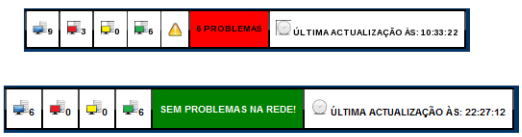

Figura 3.17 – Barra informativa do estado da rede: a) Com problemas b) Sem problemas

A outra forma de reportar os problemas é através do menu principal da aplicação, particularmente na área de problemas da rede. Nesta secção os problemas são divididos em problemas de máquina ou de recurso. Cada registo é composto pela identificação e descrição

do problema, pela localização do dispositivo onde ocorreu o problema e pela data em que foi dado o aviso. Para um maior detalhe sobre cada problema, é possível clicar em cada um dos registos. Quando tal acontece é mostrada uma janela com as características do dispositivo, detalhando o problema para que seja mais facilmente identificável pelo administrador da rede.

Figura 3.18 – Secção de problemas na rede

3.3.4. Sistema de apoio à gestão

O Athena disponibiliza um sistema de apoio à decisão orientado à gestão da rede (SAG). Este sistema, tal como o nome indica, pretende servir de ferramenta de apoio para os administradores na tarefa de gestão da rede. Numa rede composta por um elevado número de dispositivos, pode tornar-se difícil para o gestor perceber qual o nível de desempenho que esta apresenta. É então possível analisar o desempenho segundo a óptica da carga de utilização dos dispositivos que compõem a rede, já que em qualquer rede existem dispositivos que têm mais utilização que outros, ou seja, há máquinas em sobre utilização e outras em subutilização. São também analisados e estimados os custos que cada dispositivo representa potencialmente para a rede, comparados dispositivos e disponibilizada uma agenda para facilitar a organização das acções sugeridas pelo sistema.

Nos dias que correm é cada vez mais importante perceber que uma boa gestão tem definitivamente impactos positivos significativos naquilo que uma empresa poupa, evitando gastar quando for desnecessário, tanto a nível de aquisição de novos dispositivos, como a nível da energia utilizada pelos dispositivos existentes.

3.3.4.1. Análise de custos

Com esta nova solução pretende-se também intervir na área da gestão dos gastos de uma empresa, particularmente no que diz respeito à energia consumida pelos dispositivos da sua rede. Para tal, a solução Athena tem uma secção de análise de custos que pretende dotar os administradores da capacidade de estimar o custo global da rede e o custo individual de cada um dos dispositivos que a compõem.

Os custos são calculados levando em conta que na fase de inserção de um novo dispositivo é necessário e obrigatório associá-lo a um modelo de horário de funcionamento e de não funcionamento. A aplicação faz uma análise de todas as horas em que o dispositivo está ligado numa semana, de segunda-feira a domingo e com base no modelo escolhido, utilizando um valor de potência por defeito e uma taxa cobrada por kWh pré-definida, estima o gasto real desse dispositivo.

Uma breve análise na página da EDP permite perceber que uma das taxas em vigor é a de 0.09 euros (9 cêntimos) por kWh consumido (Á data de 22 Julho de 2010). Assumindo esta taxa e ainda um consumo médio de 0.25 kW por cada dispositivo, são calculados os custos estimados. É também possível personalizar a potência consumida por cada dispositivo, individualmente, bem como a taxa a aplicar no geral a todos eles, antes de se realizar o cálculo personalizado dos custos.

O custo global é calculado a partir da soma dos custos correspondentes à electricidade consumida diariamente por todos os computadores da rede, com base no modelo de horário que cada um utiliza. Posteriormente, apresentam-se os resultados sob a forma gráfica, sendo disponibilizada também a informação dos custos semanais, mensais e anuais para toda a rede, com base na sua configuração.

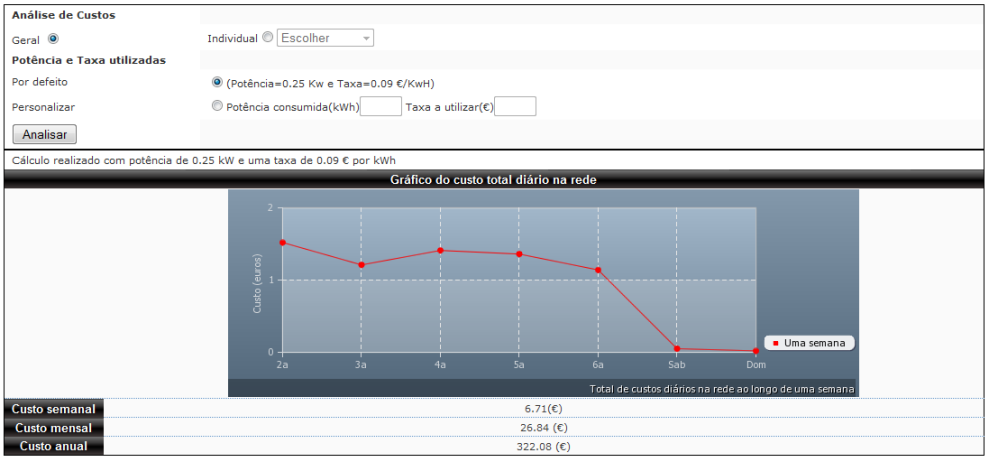

Figura 3.19 – Exemplo de análise de custo global

A área de custo individual permite que se calcule o custo associado a um dispositivo de cada vez. Este tipo de cálculo tem uma apresentação diferente do cálculo do custo global. Aqui é apresentado um gráfico dos custos diários estimados do dispositivo seleccionado, a informação dos custos semanais, mensais e anuais, e ainda uma comparação gráfica realizada com os restantes modelos de horários disponíveis no Athena. A ferramenta realiza uma análise dos custos inerentes a cada um dos modelos de horário disponíveis no sistema e identifica qual o melhor horário para utilizar, ou seja aquele cuja utilização é aconselhável para que o dispositivo gaste menos.

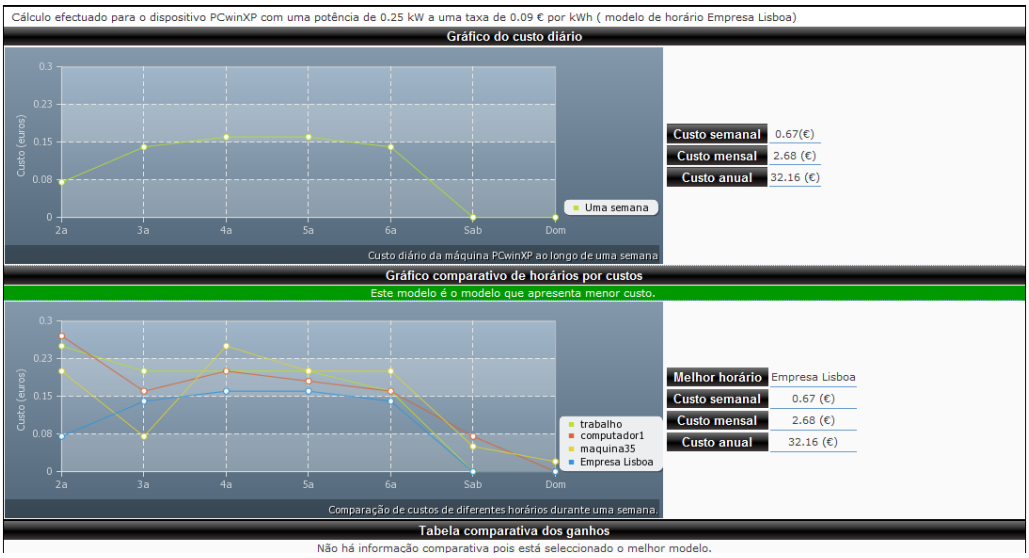

Figura 3.20 – Exemplo de análise de custo individual I

Com esta ferramenta pretende-se que o administrador possa analisar e eventualmente reajustar os horários utilizados por cada um dos dispositivos na rede, de forma a não gastar energia desnecessária.

Figura 3.21 – Exemplo de análise de custo individual II

Para fins administrativos e de controlo das acções realizadas no Athena, existe ainda um histórico com a descrição de cada uma das acções por data e hora.

3.3.4.2. Análise de desempenho

Nas outras ferramentas de monitorização, quando existe um excesso de utilização de um recurso como a carga do CPU, é gerada uma notificação. No entanto, o SAG desenvolvido permite que o administrador analise o comportamento do recurso ao longo de um período maior, que pode ser uma semana ou um mês, com base em valores médios, e perceber se de facto se tratou de uma situação anómala mas pontual ou se é uma situação que se tem repetido e que revela a necessidade de alterações mais profundas, como a aquisição de novo material ou a troca por outro que esteja numa situação de subutilização.

A secção de análise de desempenho permite analisar o sistema de duas formas distintas: globalmente ou individualmente. A nível individual é necessário escolher um dispositivo da rede, um recurso para analisar, um período para realizar a análise, incluindo a definição obrigatória de um intervalo de almoço para que o programa não contabilize os tempos mortos habituais desse período que podem por sua vez influenciar negativamente os resultados a apresentar, e escolher ainda os valores para os níveis mínimos e máximos. O sistema analisará então o comportamento do recurso escolhido e apresentará os resultados em dois formatos: tabela e gráfico. A tabela é composta pelos valores médios de utilização total, da parte da manhã e da parte da tarde, e o gráfico mostra o desempenho do recurso ao longo do período definido, o valor médio total desse recurso e ainda o nível máximo, definido pelo utilizador. Mediante estes resultados, o sistema poderá ou não gerar uma sugestão de gestão para o administrador. Se o nível de nível máximo for ultrapassado estaremos perante uma situação com excesso de utilização do recurso, caso contrário, estaremos perante uma utilização normal.

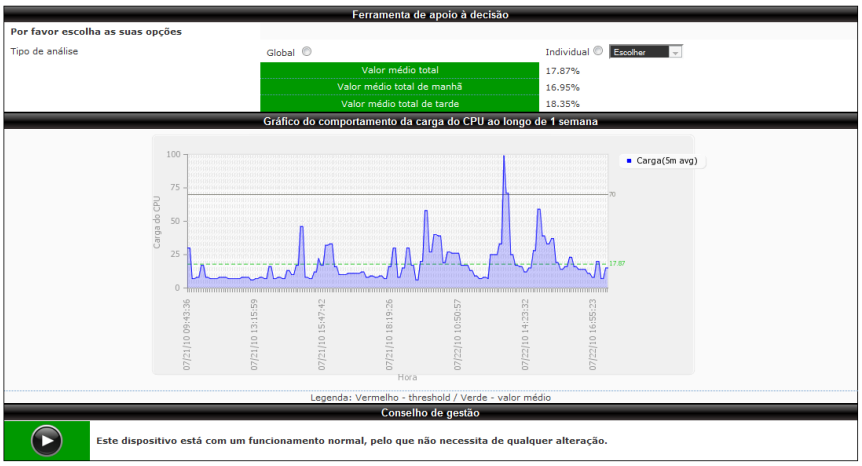

Figura 3.22 – Exemplo de utilização normal da carga do CPU (nível máximo de 70%)

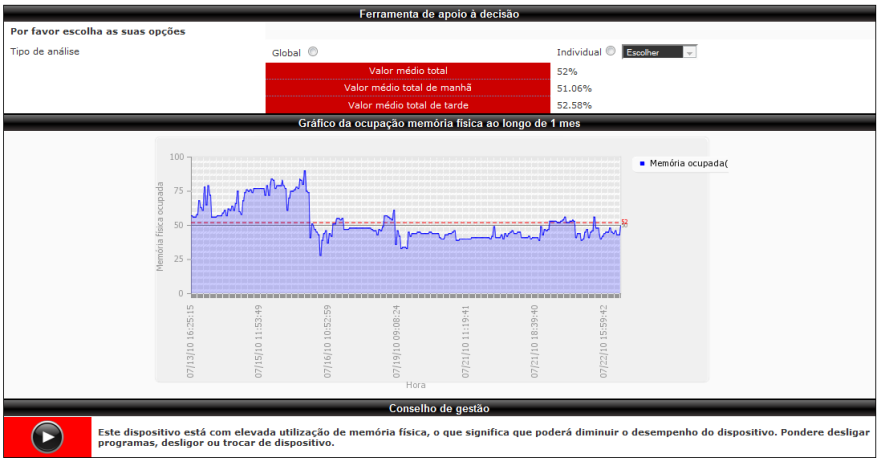

Figura 3.23 – Exemplo de utilização da memória física (nível máximo de 50%)

A nível global, é pedido um recurso para analisar, um período, com o requisito da definição do horário de almoço, e os dois níveis. O sistema analisará então o comportamento desse recurso em todas as máquinas do sistema. O resultado é apresentado de várias formas, num gráfico de barras que mostra a comparação dos valores médios do recurso obtidos para cada um dos dispositivos da rede, permitindo perceber quais deles não chegaram ao níveis mínimo pré-definido ou ultrapassaram o níveis máximo pré-definido, ou numa tabela com a mesma informação mais detalhada, onde se incluem as sugestões de gestão e ainda a opção de se adicionar dispositivos a uma agenda, que será descrita mais à frente neste capítulo.

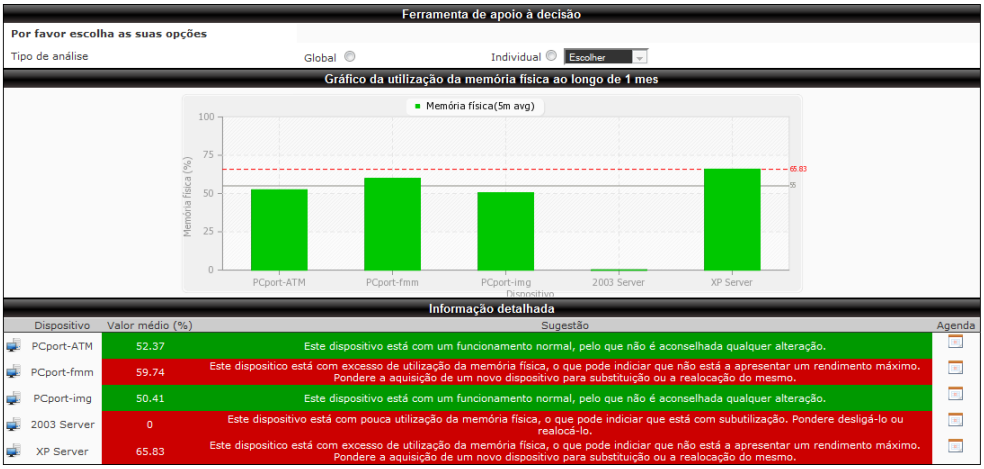

Figura 3.24 – Exemplo de uma análise de desempenho global

Sugestões de gestão

Este sistema de apoio à gestão apresenta também uma extensa lista de sugestões que visam auxiliar o gestor, consoante o estado em que se encontrem os dispositivos. Por exemplo se a utilização da carga do CPU de uma máquina, ao longo de uma semana, for excessiva, o sistema poderá sugerir que se troque essa máquina por outra que esteja numa situação contrária, ou seja com subutilização desse recurso, ou em último caso sugerir a aquisição de uma nova máquina para substituição. No caso da primeira sugestão referida, a ferramenta de

comparação de dispositivos e a agenda permitem organizar essas trocas. A seguir apresentam-se outros exemplos de sugestões para melhorar a gestão da rede:

- No caso de elevada utilização do disco rígido, aconselha-se liberar algum espaço, adicionar um novo disco ou trocar com outro com pouca utilização;

- No caso de baixa utilização da memória física, ponderar trocar as memórias com outra máquina que esteja a necessitar de a aumentar, levando sempre em conta se são compatíveis entre si.

3.3.4.3. Ferramenta de comparação de dispositivos

O sistema de apoio à gestão disponibiliza ainda uma ferramenta de comparação de dispositivos (FCD) que oferece uma série de funções com o intuito de tentar ajudar os administradores no processo de gestão e organização da rede.

Para poder usufruir da FCD, é necessário que existam entradas na agenda. Através da secção de análise de desempenho é então possível adicionar dispositivos à agenda, no caso particular de se verificarem situações críticas ou de subutilização de recursos. Para que seja adicionada uma nova entrada à agenda é preciso definir uma série de parâmetros:

- A acção a tomar;

- A data da acção;

- A prioridade da acção.

O utilizador pode escolher uma de três acções disponíveis: realocar, limpar ou desligar. Cada acção deve ser acompanhada de uma data para a realizar e de um nível de prioridade (de 1 a 10, sendo que o 1 é o mais prioritário).

Análises comparativas de dispositivos da rede

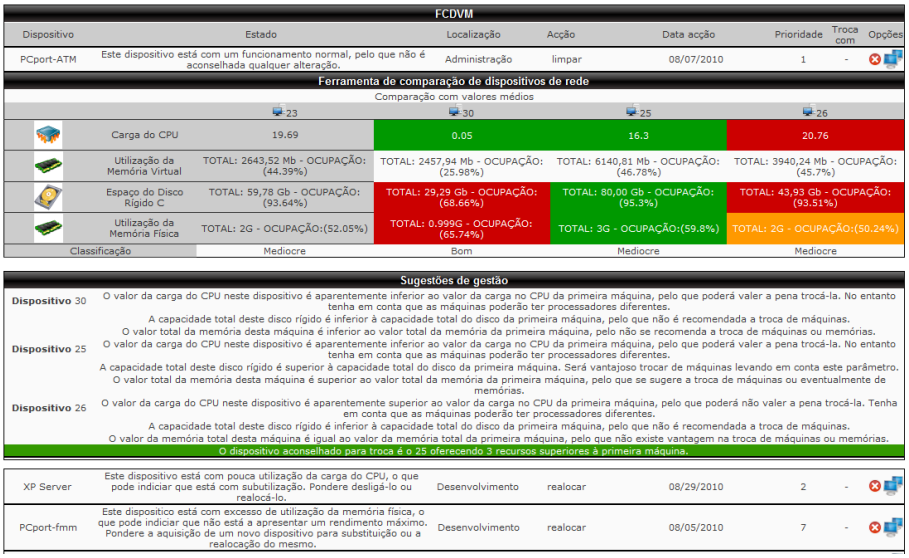

Figura 3.25 – Exemplo de comparação por valores médios na FCD

Estas análises só são possíveis quando existem pelo menos dois dispositivos na agenda, permitindo que se comparem até quatro máquinas para verificar a viabilidade de realizar a troca entre duas delas. Uma análise é composta pelas comparações dos recursos iguais entre as máquinas, um a um, e os resultados são apresentados numa compreensiva tabela de valores e numa descrição analítica dos recursos de cada máquina. Com base no resultado obtido pela comparação realizada, o sistema apresentará um parecer positivo ou negativo em relação à viabilidade da troca dos dois dispositivos. Existem dois tipos de comparações: as comparações instantâneas com base nos valores registados mais recentes, e as comparações de desempenho, com base nos valores médios registados ao longo de determinado período. Este último tipo de comparação é o ideal após a realização de uma análise de desempenho global, já que esta também lida com valores médios.

3.3.4.4. Agenda

A criação de uma agenda tem como objectivo fornecer uma maior organização à secção de análise de desempenho desta solução de monitorização. Para se inserir uma entrada na agenda é primeiro necessário realizar uma análise de desempenho global da rede, identificando quais os dispositivos que requerem atenção. Posto isto, é possível adicioná-los à agenda. Com esta agenda pretende-se que o administrador tenha um meio de planear as acções a realizar nos dispositivos da sua rede, organizando os dias em que as vai realizar, através de uma interface gráfica. Cada acção que é inserida na agenda terá uma cor que varia consoante o seu nível de prioridade, sendo que o verde mais claro é a menos prioritária e o verde mais escuro representa o maior nível de prioridade. A seguir apresenta-se uma figura que exemplifica um mês da agenda.

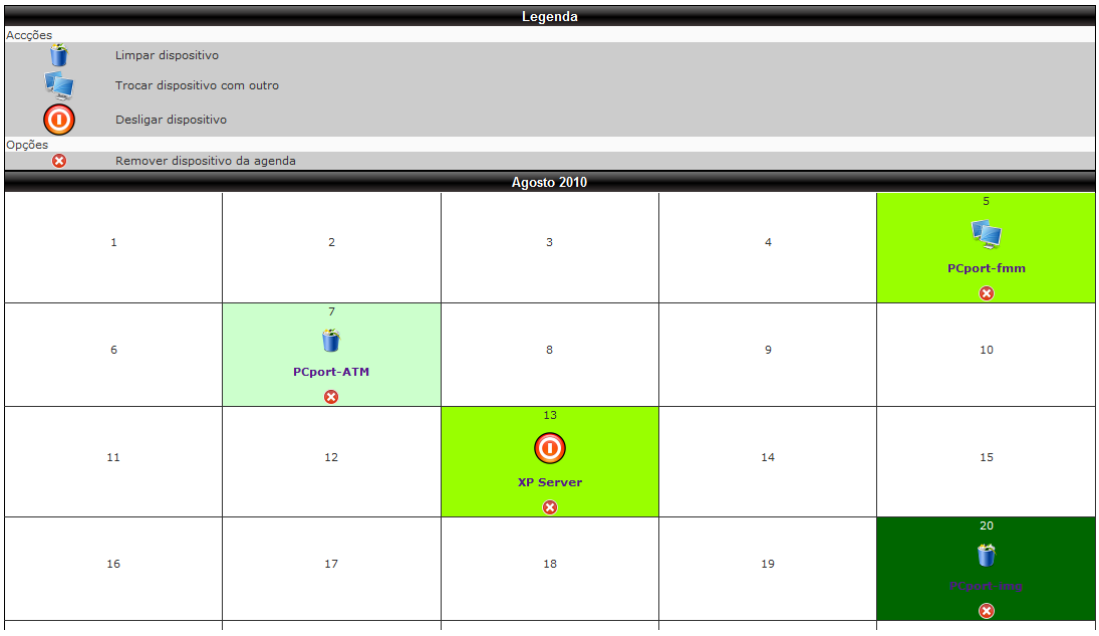

Figura 3.26 – Exemplo de um mês na agenda

Para além da sua funcionalidade, sobretudo informativa, existem ainda duas opções disponíveis na agenda. A qualquer momento é possível remover uma entrada, por exemplo quando uma acção já foi concluída, e também clicar na própria entrada para ver em maior

detalhe a sua descrição. Na figura seguinte apresenta-se um exemplo do detalhe de uma entrada.

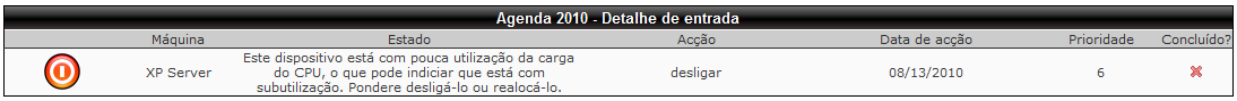

Figura 3.27 – Exemplo do detalhe de uma entrada da agenda

3.3.4.5. Classificações de estados

Para além das comparações dos recursos de cada uma das máquinas, na agenda é ainda apresentada a estimação do estado real de cada uma das máquinas, com base nos valores dos seus recursos. Cada máquina pode estar num de quatro estados possíveis, organizados do melhor para o pior:

1. Muito Bom
2. Bom
3. Medíocre
4. Muito Mau

Estes estados são calculados pela ferramenta com base nos resultados obtidos a partir da aplicação de um classificador baseado em árvores de decisão aos valores dos recursos (Ver Anexo C). Este classificador foi criado com quatro atributos:

- Ocupação da carga do CPU

- Ocupação do disco rígido C:

- Ocupação da memória virtual

- Ocupação da memória física

As classificações são executadas em duas secções. Na ferramenta de comparação de dispositivos, as classificações são aplicadas aos valores médios dos recursos e, com base nos mesmos, são atribuídos estados estimados aos dispositivos, sendo integrados nos resultados da comparação dos mesmos. É ainda possível aceder à área de classificações, onde é possível aplicar a classificação de estados de uma forma instantânea, para saber qual o estado dos dispositivos nesse momento, com base nos valores dos seus recursos nesse instante.

Capítulo 4

Apresentação e comparação de resultados

O desenvolvimento deste trabalho teve como objectivo a criação de uma nova solução de configuração e monitorização de redes que oferecesse não apenas uma maior simplicidade a nível da interacção do utilizador, para contrariar a complexidade de algumas ferramentas que acaba por esconder algumas funcionalidades que oferecem, mas também uma ferramenta que servisse de apoio à gestão de uma rede, aconselhando e auxiliando o administrador nas acções a tomar.

4.1. Arquitectura

Todas as ferramentas analisadas suportam uma arquitectura distribuída de monitorização, ou seja permitem que se defina um servidor de monitorização e servidores de recolha de informação em locais diferentes. Este tipo de arquitectura é ideal para redes constituídas por muitos dispositivos, sendo assim possível dividir a carga da recolha da informação, geralmente associada a um só servidor, por vários servidores. A solução Athena foi desenvolvida para funcionar em ambientes mais pequenos pelo que ainda não suporta este tipo de arquitectura.

4.2. Configuração

A configuração da ferramenta de monitorização Nagios não é de todo um processo rápido. No entanto, a maior parte das soluções baseadas nesta ferramenta permitem uma rápida configuração, embora não na sua totalidade. Na solução desenvolvida a configuração é ainda mais facilitada. Ao contrário da maior parte das soluções de monitorização baseadas na ferramenta anterior, as configurações efectuadas no Athena, sejam inserções de novas máquinas ou alterações dos dados existentes, são aplicadas no Nagios no momento imediato à submissão das mesmas, não sendo necessário que o utilizador execute manualmente o recarregamento da ferramenta para que as alterações entrem em vigor. Todos os ficheiros de configuração são alterados no momento em que o utilizador submete os dados e o próprio Nagios é prontamente reiniciado para o efeito. Das soluções analisadas tanto o Nconf, como o Opsview, embora permitam realizar uma extensa configuração da ferramenta, não implementam o processo de aplicação das alterações realizadas. Apenas o Centreon disponibiliza na sua interface o carregamento dos novos ficheiros de configuração no ambiente do Nagios, para que o efeito seja imediato.

As opções de configuração disponibilizadas por cada uma das ferramentas cobrem a maior parte das configurações do Nagios, sendo que o Centreon e o Opsview são das mais completas. No entanto, o facto de apresentarem todas as opções que o Nagios oferece, pode

significar que traz também alguma complexidade às suas interfaces. A inserção de um dispositivo, por exemplo, acaba por pedir ao utilizador demasiadas informações como por exemplo as propriedades de verificação, o que muitas vezes representa uma complicação deste processo. Assim, levando em conta que o Athena foi idealmente pensado para funcionar em redes pequenas, pretendeu-se oferecer ao utilizador um grau mais simples de configuração, escondendo alguma da complexidade das características de um novo dispositivo.

Para além da configuração requerida pelo Nagios, ou seja a informação relativa a cada um dos dispositivos, esta solução tem como vantagem a possibilidade de criar e associar modelos de horários de funcionamento e não funcionamento a cada um dos dispositivos, permitindo que o administrador tenha um maior controlo sobre o funcionamento dos mesmos. Juntando a estes modelos a possibilidade de definição de um número de dias durante os quais um dispositivo tem permissão para estar ausente da rede, mais os *timeperiods* escolhidos aquando das definições das notificações, este conjunto de funcionalidades representa uma mais-valia, permitindo evitar que se mostre informação de erro que diga respeito a máquinas que estejam ausentes da rede.

4.3. Apresentação

Sendo o Nagios o motor de monitorização comum entre as soluções de monitorização analisadas, incluindo a solução Athena, todas elas têm nas suas arquitecturas uma camada de utilizador que é composta por uma interface Web. As interfaces das ferramentas analisadas são igualmente compreensíveis, embora na parte da configuração possam atingir alguma complexidade dada a grande quantidade de informação apresentada. Esse facto, para quem não está ambientado com o Nagios, pode tornar-se num primeiro impacto negativo. Esta nova solução prima pela simplicidade, mesmo que na secção de configuração não ofereça tantas opções de configuração como as restantes soluções, e acaba por oferecer ao utilizador um contacto mais imediato e uma interface mais *user-friendly*.

4.4. Visualização

A visualização dos dados nas diferentes ferramentas é bastante inteligível. Tirando o Nconf que é uma ferramenta de configuração não apresentando qualquer área de visualização da informação do estado global e individual da rede, tanto o Opsview como o Centreon oferecem uma interface facilmente interpretável nesta área. Ambas as ferramentas apresentam ainda um mapa da rede, sendo que o mapa do Opsview, composto por uma imagem, é muito parecido com o mapa que o próprio Nagios disponibiliza, pelo que se pode tornar um pouco confuso se existirem muitos dispositivos na rede. Já o Centreon oferece um mapa mais interessante, desenvolvido para ser executado em Java Virtual Machine, e que possibilita que o utilizador interaja com cada dispositivo para ver a informação individual de uma forma mais detalhada.

Uma das formas encontradas para apresentar a informação da rede de uma forma mais simples e clara, com esta nova solução Athena, é a possibilidade de visualizar os estados actuais dos recursos das máquinas no formato gráfico, para além das habituais tabelas informativas. A informação neste formato é apresentada em gráficos de barras ou do tipo *pie*, representando os estados instantâneos dos recursos. Esta opção pretende facilitar a gestão, evitando que o administrador tenha que analisar detalhadamente a informação das tabelas. Com as restantes ferramentas, o Opsview e o Centreon, esta representação gráfica dos estados actuais não existe, sendo utilizados nesta área os mesmos gráficos de desempenho, que são utilizados nas habituais áreas de análise da rede.

A organização oferecida pelo Athena é também das mais acessíveis e perceptíveis. Em vez de disponibilizar um mapa confuso da rede, como por exemplo o do próprio Nagios, o Athena possibilita a criação de salas representando salas reais, permitindo que se faça o mapeamento das posições virtuais com as posições reais. Assim, é possível identificar mais facilmente a localização dos dispositivos para os casos em que existem alertas de problemas, ajudando a reduzir o tempo de resolução dos mesmos, e para os casos em que o utilizador pretenda trocar dois dispositivos, depois de ter realizado uma comparação de dispositivos e consultado a agenda de acções da solução. Este mapa da rede permite também uma maior interacção por parte do utilizador, sendo possível ver a informação individual detalhada de cada componente da rede, tal como o Centreon.

Nesta nova solução existe uma secção de estado de rede onde é possível observar a informação global da rede de uma forma concisa. A informação disponibilizada permite ver:

- Distribuição das máquinas por estados;

- Gráfico de composição da rede;

- Gráfico com a distribuição das máquinas por sistemas operativos;

- Gráfico com a distribuição dos serviços por estado.

É ainda possível ver o estado global da rede, dividido por estado de máquinas e estado de serviços, registados na última hora.

Ainda no campo da visualização de informação, as ferramentas Opsview e Centreon disponibilizam secções de *Business Intelligence*. No caso da primeira, com recurso aos Jasper Reports que permitem descarregar ficheiros do tipo *pdf* com a informação sintetizada do estado da rede e dos seus componentes, embora estes relatórios não estejam disponíveis na versão gratuita da solução, mas apenas através da instalação das respectivas extensões comerciais. Em relação à segunda, existe um módulo designado por Centron BI, já integrado na solução, que permite a criação de relatórios personalizados de disponibilidade e desempenho da rede, com destaque para a possibilidade de se agendar a criação automática dos relatórios. Em qualquer dos casos, esta opção é uma mais-valia para os administradores, visto que permite criar documentação sobre a própria rede para consulta e futura análise. Tanto o Nconf como o Athena não dispõem de uma secção deste tipo, sendo que no caso da nova solução esta é uma área a desenvolver como trabalho futuro.

4.5. Análise do comportamento da rede

A análise do comportamento da rede é uma das áreas mais importantes de uma ferramenta de monitorização. Esta área pode ser bastante extensa, mas no geral diz respeito à representação gráfica do desempenho dos dispositivos da rede, existindo diversos modos de realizar esta representação. O Centreon utiliza o motor RRDTool para armazenar os dados de uma forma eficiente e criar uma grande variedade de tipos de gráficos. Já o Opsview utiliza o Flot, uma biblioteca de criação de gráficos baseados na linguagem *javascript* que oferece várias opções de personalização e uma curiosa opção de *zoom*, que permite que se amplie uma certa zona do gráfico para ver a informação em maior detalhe. No desenvolvimento da nova solução foi adoptada uma biblioteca de gráficos em *php* chamada de pChart. A partir dela é possível criar vários tipos de gráficos, todos eles totalmente personalizáveis, e com um visual bastante simples e atractivo, para uma melhor compreensão por parte do utilizador. A escolha deste tipo de gráficos, em vez do RRDTool, prende-se com a exagerada quantidade de informação presente num gráfico criado por este último. Optou-se em vez disso por um tipo de gráfico mais simples, que se centra mais no próprio gráfico do que na informação extra ao seu redor. No entanto, essa informação extra não é esquecida na nova solução, sendo disponibilizada numa área complementar, no formato de tabelas. Não obstante a razão apresentada para não se ter optado pelo RRDTool, fica como trabalho futuro a implementação deste motor para armazenamento de dados, já que este tem a vantagem de compactar o tamanho das bases de dados e impedir que as mesmas cresçam exponencialmente com os dados armazenados.

A área de análise do comportamento na rede, na maior parte das ferramentas de monitorização, é normalmente dada pelos gráficos de desempenho anteriormente mencionados. No entanto, a solução Athena disponibiliza outras áreas que têm o objectivo de permitir acompanhar e analisar o desempenho da rede ao longo do tempo de uma forma diferente e que se pretende que mais proveitosa. Uma dessas áreas é a área de comparação de recursos, inexistente nas outras ferramentas. A partir dela é possível ver quais os dispositivos que têm mais utilização nos principais recursos, num determinado instante. Este processo pode ser realizado de uma forma global, onde são comparados os valores dos recursos de todos os dispositivos, com um gráfico por serviço, ou individualmente sendo possível escolher quais os dispositivos a comparar. Com esta ferramenta pretende-se dotar o administrador da capacidade de antever situações críticas, sendo possível detectar, por exemplo, quando a percentagem da utilização de um recurso se aproxima de um valor crítico.

Sistema de apoio à gestão

Nas ferramentas analisadas, a área de sistemas de apoio à decisão não revelou estar presente de forma alguma. Para oferecer algo nesta área, o desenvolvimento desta nova solução teve também como objectivo criar e disponibilizar um sistema deste tipo que auxilie o administrador na tarefa de gerir a sua rede. Esse sistema é composto por várias secções: a análise de custos, a análise de desempenho, a comparação de recursos, a agenda e a classificação dos estados dos dispositivos da rede.

Análise de custos

Sabendo como é importante a gestão dos gastos numa empresa, outra das características interessantes é a preocupação com os gastos que o funcionamento de uma rede pode representar, pretendendo disponibilizar funcionalidades de apoio à gestão desses mesmos custos.

Para tal o Athena oferece um conjunto de conceitos, composto pelas notificações, pelos modelos de horários de funcionamento e de não funcionamento e pelos dias de ausência permitida da rede, que pretende representar uma mais-valia nesta gestão, já que assim é possível gerar alertas quando as máquinas funcionam fora dos períodos que estão definidos. Assim é possível garantir que não há um gasto suplementar àquele previsto e se o houver os alertas avisam o administrador para que se resolva a situação e se evite continuar a consumir electricidade desnecessariamente. Existe ainda uma secção de análise de custos que tem como objectivo permitir fazer uma estimativa do quanto gasta, no total, a rede por dia, por semana, por mês e por ano, mediante os modelos de horários de funcionamento e não funcionamento escolhidos para cada máquina, de forma a apoiar o administrador na sua tarefa de reavaliação dos dispositivos da sua rede, dando uma noção se de facto vale a pena que todas as máquinas esteja a funcionar com cada um dos modelos de horários que têm nesse momento associados. Esta área pretende ajudar nessa tarefa com a análise individual do gasto de cada máquina, permitindo que o administrador obtenha uma estimativa de quanto cada uma delas gasta nos períodos já mencionados, e comparando ainda o seu modelo de horário com os restantes modelos para indicar se o modelo actual é o mais indicado na rede ou se existe outro potencialmente melhor. Os resultados apresentados são meramente estimativas, dado que os dispositivos têm potências diferentes e que a taxa por kWh não é certa. No entanto esta área não deixa de representar um esforço, e uma ideia, no sentido de se melhorar a gestão dos gastos que uma rede pode apresentar. Nas ferramentas analisadas não existe qualquer secção semelhante.

Análise de desempenho

Nas ferramentas analisadas o utilizador pode visualizar o comportamento dos recursos ao longo de um período, e ter uma ideia do seu desempenho com a mera observação de um gráfico. Nesta nova solução a possibilidade de fazer uma análise de desempenho, seja individual ou global, constitui uma tentativa de tornar um gráfico de desempenho mais informativo e útil para o administrador. O cálculo dos valores médios de utilização nas análises individuais permite perceber, por exemplo, como é a distribuição da utilização de um determinado dispositivo ao longo de um determinado período, se é mais utilizado da parte da manhã, da parte da tarde, ou se é uma utilização uniforme ao longo do dia, e se ultrapassa um *threshold* crítico definido pelo utilizador. A partir desta análise o administrador poderá reavaliar o estado e a localização de um dispositivo dentro da empresa.

A nível global, esta ferramenta tem a vantagem de permitir comparar a utilização de um recurso comum entre os dispositivos da rede ao longo de um período, de forma a poder

informar o administrador sobre quais os dispositivos que estão com utilização a mais ou a menos de determinado recurso. Esta análise global permite que o administrador possa ter uma noção da evolução da sua rede, podendo detectar quais os seus pontos fracos, ou seja, as máquinas que podem de alguma maneira comprometer o desempenho geral da rede. O Athena não só permite identificar esses pontos fracos como disponibiliza duas ferramentas, uma para comparação de máquinas e outra para agendamento de acções, com o objectivo de facilitar o processo. Caso se verifique que o estado de um dispositivo não é o ideal, é possível agendar acções para repor a normalidade através da agenda da solução. Essa é outra das diferenças desta nova solução em relação às outras. O objectivo da criação de uma agenda é reunir a informação dos dispositivos com sobre e subutilização de recursos na rede, oferecendo a possibilidade de agendar acções, com prioridades, para resolver as situações, tentando assim dar ao administrador uma visão global e mais detalhada da rede, ao mesmo tempo que oferece uma ferramenta de organização para ajudar nas alterações a efectuar. Por fim, a possibilidade de gerar comparações entre os dispositivos da agenda, com sugestões de gestão incluídas, permite, por exemplo, que o administrador, analise os recursos de dois dispositivos que pretenda utilizar numa troca e receba conselhos sobre a viabilidade dessa mesma troca.

Classificação de estados

No que diz respeito ao estado de um dispositivo, em todas as ferramentas de monitorização analisadas esse estado é dado pela avaliação da sua disponibilidade instantânea, ou seja, se está ligado, desligado ou ausente da rede, ou então através dos estados individuais instantâneos de cada um dos recursos a ele associado. Através da utilização de um classificador baseado em árvores de decisão, esta nova solução permite estimar o estado real de um dispositivo, com base na análise dos valores médios de utilização de quatro recursos diferentes, a carga do cpu, o disco rígido, a memória física e a memória virtual.

Esta capacidade de estimar os estados reais dos dispositivos permite que o administrador tenha uma ideia do eventual desgaste que as máquinas da sua rede poderão estar a sofrer, já que muitas vezes quando surge um problema numa máquina, pode parecer apenas um problema isolado, quando de facto pode ser um sintoma de que potenciais maiores problemas poderão surgir nessa mesma máquina a curto prazo. Esta funcionalidade visa portanto ajudar na antecipação de problemas graves, suscitando a tomada de uma acção na máquina que está, aparentemente, mais debilitada.

Capítulo 5

Conclusões e trabalho futuro

É incontestável que a evolução tecnológica tem mudado a forma de actuar da maior parte das empresas, permitindo inclusivamente que se começasse a monitorizar o comportamento das suas redes de uma forma automática, mais rápida e detalhada do que anteriormente. Actualmente são tantas as ferramentas de monitorização disponíveis, que se pode dizer que uma empresa que não faça uso de uma delas, é uma empresa que está a perder terreno para as suas mais directas concorrentes.

O desenvolvimento de uma nova solução de monitorização baseada no Nagios revelou ser um desafio interessante com objectivos complicados para atingir, principalmente tendo em conta o número de ferramentas de monitorização disponíveis e estabelecidas no mercado há alguns anos. Após um detalhado estudo da oferta existente, delineou-se um formato para a nova solução, com o planeamento em detalhe de cada uma das suas áreas e do que se podia oferecer de útil e diferente.

Após o estudo de diversa bibliografia sobre monitorização e gestão de redes, chegou-se à conclusão que a maior parte das ferramentas actuam principalmente no campo da monitorização de redes, disponibilizando também algumas opções para analisar os seus desempenhos. É certo que se monitorizam as máquinas, se apresentam os resultados e se disponibilizam meios para corrigir ou evitar problemas, mas existe uma falha na assistência que se podia prestar aos administradores que gerem as redes de empresas. Como tal, a nova solução Athena apresenta-se como uma ferramenta de monitorização que vem tentar implementar algumas ideias, disponibilizando algumas funcionalidades nesse sentido.

A primeira etapa no desenvolvimento consistiu na garantia das funcionalidades básicas de uma ferramenta de monitorização. De seguida foram estudadas funcionalidades na área da gestão de redes e entendeu-se como mais-valia o desenvolvimento de um sistema de apoio à decisão orientado à gestão de uma rede. A ideia de um sistema de apoio à decisão, porém, partiu do princípio que um sistema deste tipo deve funcionar como guia de gestão para um administrador de redes, fornecendo informações e sugestões que suportem as suas acções, mas não tentando fornecer respostas definitivas sobre as acções a tomar dado que a informação poderá nem sempre ser totalmente precisa, necessitando sempre da validação do utilizador. O resultado foi uma nova solução que permite monitorizar, visualizar a informação recolhida e analisar desempenhos, e que tenta apoiar a gestão da rede com base nos dados reais desta.

A ideia de criar uma secção de análise de desempenho da rede, integrando-a com uma ferramenta de comparação de dispositivos, com conselhos para a gestão e ainda com uma agenda de acções, foi uma forma de aproveitar as potencialidades dos dados recolhidos sobre a rede, com o objectivo de criar um sistema de apoio à decisão orientado à gestão de uma rede. Não sendo ainda uma área definitivamente concluída a nível do desenvolvimento, torna-

se num primeiro passo na direcção de verdadeiros sistemas de apoio à gestão de redes de dispositivos.

No entanto, e como em qualquer nova aplicação, há sempre trabalho futuro a desenvolver.

Uma das propostas para desenvolvimento futuro é conseguir implementar uma arquitectura distribuída de monitorização, com base nas potencialidades do Nagios, e disponibilizar uma área de configuração da mesma, à semelhança do que é feito na ferramenta NConf, de forma a poder aplicar esta solução a meios compostos por um grande número de dispositivos sem ter o problema do excesso de carga no servidor principal.

Outra funcionalidade que poderá ser estudada é a possibilidade de se criar um mecanismo que instale e configure automaticamente, de uma forma remota, os agentes de monitorização nos dispositivos que se pretendem monitorizar, para que não seja preciso delegar em alguém essa tarefa, que poderá ser morosa, tanto mais quantos mais forem os dispositivos que compõem a rede. Esta funcionalidade deverá ser implementada antes de se implementar a arquitectura distribuída que foi referida.

A expansão do número e tipo de recursos e serviços que podem ser monitorizados será outra forma de enriquecer a aplicação. A ideia será monitorizar serviços de rede e acrescentar mais e diferentes verificações de recursos às existentes, como por exemplo monitorizar *software* para analisar se as licenças são válidas, monitorizar impressoras para detectar se há falta de papel ou se o cartucho está quase vazio. Ainda neste campo, e aproveitando o conceito de *plug-ins* do Nagios, poderá ser interessante desenvolver uma área que possibilite adicionar novos *plug-ins* de uma forma rápida e simples para o utilizador.

No que diz respeito à forma como são armazenados os dados recolhidos, uma das melhorias que será interessante implementar é a adopção do motor *RRDTool*, bem conhecido pelo seu excelente desempenho, não só na área da representação gráfica, como no armazenamento de dados, permitindo compactar a informação. A ideia será utilizá-lo somente para esta última função, já que a nível da representação gráfica a actual opção, dada a sua simplicidade e facilidade de interpretação, é a ideal.

Outra área que será desenvolvida no Athena será a área de *Business Intelligence*. O objectivo será enriquecer a solução disponibilizando informação concisa em relatórios criados no formato pdf. Ainda nesta área, existe o objectivo de possibilitar o envio de uma *newsletter* para os administradores, com período configurável pelo utilizador, com uma síntese do comportamento da rede e de todos os seus componentes.

O sistema de apoio à decisão orientada à gestão de redes é outra das áreas que deverá sofrer uma extensão de funcionalidades no futuro. Sendo uma área pouco explorada nas ferramentas de monitorização existentes, tem ainda muito trabalho para desenvolver, embora levando sempre em conta que uma área de apoio à gestão deverá funcionar sempre como uma ferramenta de apoio e não como ferramenta de respostas. Para tal deverão ser estudadas todas as vantagens e contrariedades da implementação de tal sistema nesta área e ainda ser analisados casos de estudo, com recurso à bibliografia de sistemas de apoio à decisão que são actualmente aplicados a outras áreas, como a medicina [14], por exemplo.

No que diz respeito à interacção do utilizador com a solução, será interessante desenvolver um acesso ao Athena a partir de dispositivos móveis. Mesmo com a noção de que não será fácil garantir as mesmas funcionalidades que se disponibilizam a partir de uma interface Web que é executado num *browser* de um computador, será possível permitir visualizar o estado dos dispositivos e serviços, os problemas na rede, e eventualmente poderá pensar-se em criar um acesso à agenda de acções para que o utilizador possa programar acções remotamente.

Anexo A

Ficheiros de configuração do *Nagios*

O funcionamento do Nagios tem por base diversos ficheiros de configuração. Todos estes ficheiros são bastante compreensíveis e facilmente editáveis. Existem vários tipos de ficheiros de configuração, os de dispositivos, os de contactos, os de períodos de tempo, os de modelos, entre outros. De seguida são apresentados alguns exemplos contemplando suas estruturas.

Definição de dispositivos

Este tipo de ficheiro de configuração é utilizado para definir os computadores de uma rede que vão ser monitorizados no Nagios. Geralmente cada tipo de computador ou dispositivo tem um ficheiro de configuração próprio, denominado de Windows.cfg ou Linux.cfg ou printer.cfg, mas no caso desta nova solução optou-se por um ficheiro de configuração comum para as máquinas com sistemas operativos Windows e Linux. A seguir apresenta-se um exemplo da definição de um dispositivo, neste caso um computador com o sistema operativo Windows.

```
define host{
        use                     windows-server;
        host_name               PCWin7;
        alias                   PC Joao Simoes   ;
        address                 192.168.2.1;
        check_period            HorarioNotificacoes;
        contacts                JoaoSimoes ;
        notification_interval   45;
        notification_period      HorarioNotificacoes;
        notification_options    d,r;       }
```

A definição de um dispositivo é composta por várias directivas, mas no Athena são utilizadas apenas as que se descrevem na tabela seguinte.

Directiva	Descrição
use	define qual o *template* que o dispositivo está a utilizar
host_name	nome que identifica o dispositivo
alias	descrição do dispositivo
address	define o endereço associado ao dispositivo. Pode ser um endereço IP ou o próprio nome do dispositivo desde que o DNS funcione.
check_period	define o nome do *timeperiod* a usar para as verificações e notificações
contacts	define quais os contactos que deve ser notificados em caso de problemas na rede
notification_interval	define o tempo, em minutos, que se espera antes de enviar outra notificação
notification_period	define o período durante o qual podem ser enviadas notificações para os contactos
notification_options	define as opções para envio de notificações. No Athena são usadas duas, a **d** que representa o envio de notificações quando um dispositivo está no estado DOWN e a **r** que representa o envio de notificações quando um dispositivo recupera de um problema

Tabela A.1 - Directivas utilizadas na definição de um novo dispositivo

Definição de serviços

A definição dos serviços é feita no mesmo ficheiro de configuração onde se definem os dispositivos, para que o Nagios possa ler a informação sequencialmente. Os serviços podem ser de vários tipos, sendo que na solução Athena são os recursos que se pretendem monitorizar e que estão associados a dispositivos. A seguir apresenta-se um exemplo da definição de um serviço, neste caso

```
define service{

        use                     generic-service
        host_name               Maquina20
        service_description     Physical Memory
        check_command           check_mem!80!90

        }
```

A definição de um serviço é composta por várias directivas, mas no Athena são utilizadas apenas as que se descrevem na tabela seguinte.

Directiva	Descrição
use	define qual o *template* que o dispositivo está a utilizar
host_name	nome que identifica o dispositivo
service_description	descrição do serviço
check_command	comando utilizado para realizar a verificação do serviço

Tabela A.2 - Directivas utilizadas na definição de um novo serviço

Definição de períodos de tempo

A definição dos períodos de tempo é feita num ficheiro de configuração criado para o efeito. Estes períodos de tempo representam os horários escolhidos pelos utilizadores durante os quais são aceites verificações e notificações referentes aos seus dispositivos. A seguir apresenta-se um exemplo da definição de um período de tempo.

```
define timeperiod{

    timeperiod_name     HorarioNotificacoes
    alias               Timperiod HorarioNotificacoes
    sunday              18:00-21:00
    monday              10:00-18:00
    tuesday             09:00-19:00
    wednesday           09:00-18:00
    thursday            11:00-20:00
    friday              12:00-23:00
    saturday            21:00-00:00

    }
```

A definição de um período de tempo é composta por várias directivas que se apresentam e descrevem na tabela seguinte.

Directiva	Descrição
timeperiod_name	Define o nome utilizado para identificar o período de tempo, para que possa ser utilizado na definição de um dispositivo ou serviço
alias	Define a descrição do período de tempo
[weekday]	Define as directivas weekday que representam o horário a utilizar para cada dia da semana

Tabela A.3 - Directivas utilizadas na definição de um novo período de tempo

Definição de contactos

A definição dos contactos é feita num ficheiro de configuração criado para o efeito. Estes contactos são utilizados para enviar notificações, se a configuração assim o permitir, para os utilizadores responsáveis. A seguir apresenta-se um exemplo da definição de um contacto.

```
define contact{

    contact_name        Joao Simoes
    use                 generic-contact
    alias               Contacto de JoaoSimoes
    email               correioelectronico@hotmail.com

    }
```

A definição de um contacto é composta por várias directivas. Na tabela seguinte apresentam-se aquelas utilizadas no Athena.

Directiva	Descrição
contact_name	Define o nome utilizado para identificar contacto
use	Define a utilização de um modelo genérico de contactos
alias	Define uma descrição para o contacto
Email	Define o correio electrónico do contacto

Tabela A.4 - Directivas utilizadas na definição de um novo contacto

Definição de modelos

A definição de modelos no Nagios permite poupar tempo na definição de novos dispositivos na rede, desde que estes tenham em comum as características definidas nas directivas de um determinado modelo. Porém, convém realçar que se for especificada uma directiva na definição de um dispositivo que também está especificada no modelo que este usa, a directiva da definição do objecto substitui a directiva do modelo. Com este facto é possível personalizar as características de cada novo dispositivo. Os modelos utilizados podem ser modelos de máquinas com Windows, modelos de máquinas com Linux, modelos de *routers*, modelos de impressoras, entre outros. A seguir apresenta-se um exemplo da definição de um modelo de uma máquina com Windows.

```
define host{

        name                            windows-server
        use                             generic-host
        check_period                    24x7
        check_interval                  5
        max_check_attempts              10
        check_command                   check-host-alive
        notification_period             24x7
        nightnotification_interval      30
        minutesnotification_options     d,r
        contact_groups                  admins
        hostgroups                      windows-servers
         register                       0

        }
```

A definição de um modelo é composta por várias directivas. Na tabela seguinte apresentam-se aquelas utilizadas no Athena.

Directiva	Descrição
name	Define o nome do modelo
use	Define a utilização de outro modelo, permitindo assim criar modelos encadeados
Check_period	define o nome do *timeperiod* a usar para as verificações e notificações
Check_interval	define o tempo, em minutos, entre as verificações efectuadas
Max_check_attempts	define o número máximo de verificações a efectuar antes de se considerar a existência de um problema
Check_command	define o comando utilizado para fazer a verificação se um dispositivo está ligado, no caso do exemplo acima
notification_interval	define o tempo, em minutos, que se espera antes de enviar outra notificação
notification_period	define o período durante o qual podem ser enviadas notificações para os contactos
notification_options	define as opções para envio de notificações. No Athena são usadas duas, a **d** que representa o envio de notificações quando um dispositivo está no estado DOWN e a **r** que representa o envio de notificações quando um dispositivo recupera de um problema
hostgroups	Define o grupo de dispositivos a que o modelo pertence
register	Define se a definição é de um modelo ou de um dispositivo. Se tiver o valor 0 então é considerado um modelo, se tiver o valor 1 é um dispositivo

Tabela A.5 - Directivas utilizadas na definição de um novo modelo

Anexo B

Base de dados da solução Athena

A base de dados da solução Athena é composta por doze tabelas. Nessas tabelas é guardada, entre outras coisas, a informação das máquinas, dos serviços, e do desempenho destes.

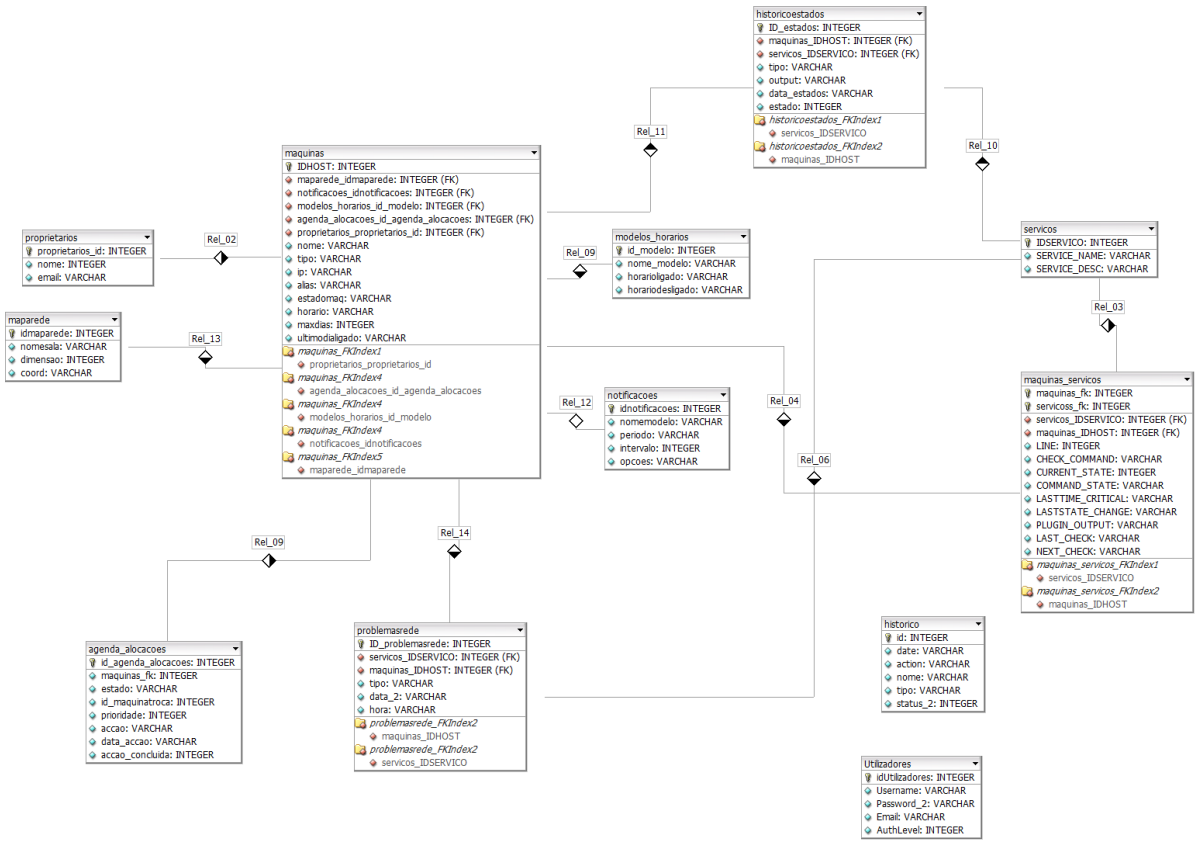

Figura B.1 – Modelo Entidade-Relação da base de dados do Athena

Anexo C

Classificador baseado em árvores de decisão

Para determinar o estado dos dispositivos da rede, foi criado um classificador com base em árvores de decisão, com a ajuda do programa CART.

De um conjunto de 450 exemplos formou-se um conjunto de treino constituído por 300 exemplos e um conjunto de teste constituído por 150 exemplos.

Posteriormente, a partir do CART, foi lida a informação do ficheiro de Excel com a tabela com o conjunto de treino. A configuração do novo modelo de classificação foi realizada com quatro atributos:

- Carga do CPU;

- Disco rígido C;

- Memória virtual;

- Memória física.

Definiu-se ainda uma classe denominada de estado, representando o estado em que o dispositivo se encontra e tendo um de quatro valores possíveis, muito bom (c1), bom (c2), medíocre (c3) e muito mau (c4). Para a variável da classe foram utilizados quatro níveis e um valor mínimo de um. O tipo de árvore seleccionado foi de classificação. Criou-se assim a árvore de decisão que se apresenta de seguida

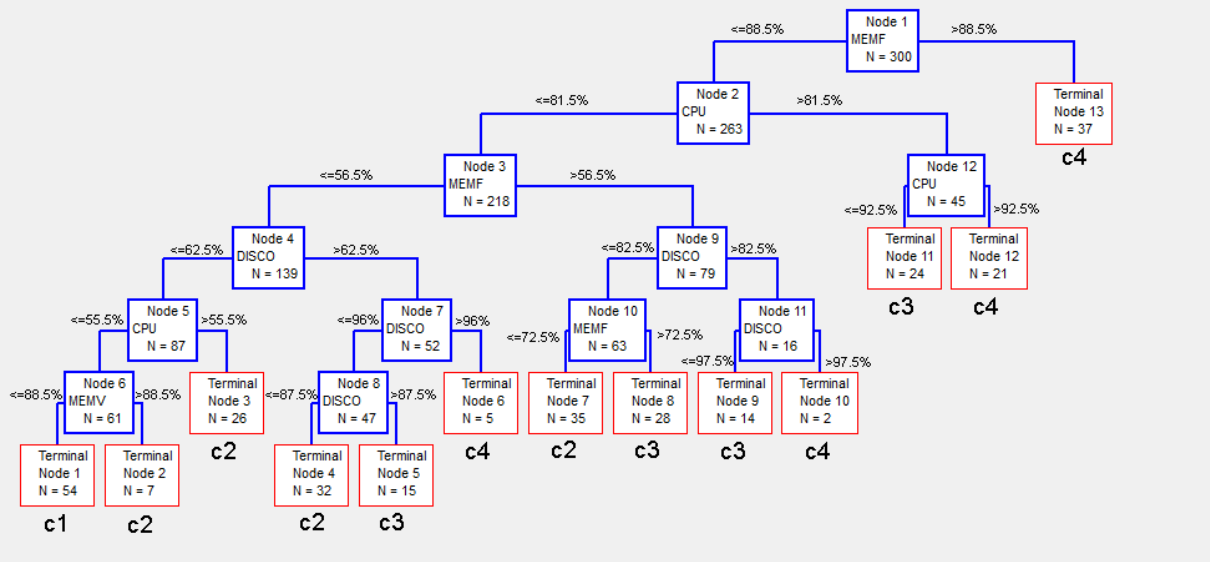

Figura C.1 – Exemplo de classificador baseado numa árvore de decisão

Esta árvore de decisão pode também ser representada de outra forma, através das regras.De seguida apresentam-se essas mesmas regras, que definem as condições que classificam os estados dos dispositivos.

```
/*Terminal Node 1*/
if
(
   MEMF <= 56.5 &&
   DISCO <= 62.5 &&
   CPU <= 55.5 &&
   MEMV <= 88.5
)
{
   terminalNode = -1;
   class = 1;
}

/*Terminal Node 2*/
if
(
   MEMF <= 56.5 &&
   DISCO <= 62.5 &&
   CPU <= 55.5 &&
   MEMV > 88.5
)
{
   terminalNode = -2;
   class = 2;
}

/*Terminal Node 3*/
if
(
   MEMF <= 56.5 &&
   DISCO <= 62.5 &&
   CPU > 55.5 &&
   CPU <= 81.5
)
{
   terminalNode = -3;
   class = 2;
}

/*Terminal Node 4*/
if
(
   CPU <= 81.5 &&
   MEMF <= 56.5 &&
   DISCO > 62.5 &&
   DISCO <= 87.5
)
{
   terminalNode = -4;
   class = 2;
}

/*Terminal Node 5*/
if
(
   CPU <= 81.5 &&
   MEMF <= 56.5 &&
   DISCO > 87.5 &&
   DISCO <= 96
)
{
   terminalNode = -5;
   class = 3;
}

/*Terminal Node 6*/
if
(
   CPU <= 81.5 &&
   MEMF <= 56.5 &&
```

```
    DISCO > 96
)
{
    terminalNode = -6;
    class = 4;
}

/*Terminal Node 7*/
if
(
    CPU <= 81.5 &&
    DISCO <= 82.5 &&
    MEMF > 56.5 &&
    MEMF <= 72.5
)
{
    terminalNode = -7;
    class = 2;
}

/*Terminal Node 8*/
if
(
    CPU <= 81.5 &&
    DISCO <= 82.5 &&
    MEMF > 72.5 &&
    MEMF <= 88.5
)
{
    terminalNode = -8;
    class = 3;
}

/*Terminal Node 9*/
if
(
    CPU <= 81.5 &&
    MEMF > 56.5 &&
    MEMF <= 88.5 &&
    DISCO > 82.5 &&
    DISCO <= 97.5
)
{
    terminalNode = -9;
    class = 3;
}

/*Terminal Node 10*/
if
(
    CPU <= 81.5 &&
    MEMF > 56.5 &&
    MEMF <= 88.5 &&
    DISCO > 97.5
)
{
    terminalNode = -10;
    class = 4;
}

/*Terminal Node 11*/
if
(
    MEMF <= 88.5 &&
    CPU > 81.5 &&
    CPU <= 92.5
)
{
    terminalNode = -11;
    class = 3;
}

/*Terminal Node 12*/
if
(
    MEMF <= 88.5 &&
```

```
    CPU > 92.5
)
{
    terminalNode = -12;
    class = 4;
}

/*Terminal Node 13*/
if
(
    MEMF > 88.5
)
{
    terminalNode = -13;
    class = 4;
}
```

Anexo D

Tutorial de instalação do NSClient++

Neste anexo apresentam-se os passos necessários para instalação do NSClient++.

1 . Fazer download da versão 0.36 do agente NSClient++ na sua versão compactada em zip.

2. Descompactar para a directoria *C:\NSClient++*. Abrir uma linha de comandos (*Start>Run->cmd*). Aceder à directoria do NSClient++ (*cd C:\NSClient++*)

3. Executar os seguintes comandos:

nsclient++ /install
nsclient++ systray

4. Abrir os serviços do Windows (*Start->Run->services.msc*), localizar o serviço NSClientpp, clicar duas vezes, aceder à aba Log On e marcar a opção – *Allow service to interact with desktop*. Fazer Ok em todas as janelas. Não iniciar ainda o serviço.

5. Copiar os ficheiros counters.defs e nsc.ini dados, para a directoria C:\NSClient++, substituindo os que lá estão.

6. Adicionar as seguintes excepções à firewall do Windows:

TCP 12489
TCP 5666

7. Activar a partilha de ficheiros e impressoras.

- Para Windows XP: Aceder ao Meu Computador e do lado esquerdo carregar em Shared Documents. Clicar com o botão do lado direito dentro dessa directoria e escolher Properties. Aceder ao separador Sharing e fazer o Wizard para activar a partilha.

-Para Windows Vista/Windows 7: Do lado direito clicar com o botão do lado direito em cima da ligação (seja ela com ou sem fios) e escolher Open Network and Sharing Center. Depois na janela que abre escolher Choose homegroup and sharing options e depois Change Advanced Sharing Settings. Escolher Public (current profile) e aí fazer as seguintes alterações:

- Turn On network discovery
- Turn On File and Printer Sharing

Fazer OK em todas as janelas.

8. Aceder novamente aos serviços, clicar com o botão do lado direito sobre o NSClientpp e escolher Restart. O cliente NSClient++ está agora instalado e activo no computador.

Agradecimentos

O desenvolvimento deste trabalho só foi possível com o apoio de algumas pessoas, sem as quais os objectivos propostos teriam sido bem mais complicados de cumprir.

Ao Prof. José Manuel Fonseca, orientador desta tese, pela sugestão do tema, pelo apoio, colaboração e estímulo proporcionados ao longo de todo o percurso.

Ao Prof. André Mora pela disponibilidade e colaboração prestada ao longo do trabalho.

À Engª Inês Mora e ao Engº Fernando Moitinho pela possibilidade de utilizar os seus computadores para testar a nova solução, em os quais seria impossível melhorá-la.

Ao Departamento de Engenharia Electrotécnica pela formação que me deu ao longo do curso e à UNINOVA pelas condições de trabalho que me ofereceram.

Aos meus colegas de curso, em especial aos meus colegas de tese Bruno Rodrigues e Rogério Rebelo, pela paciência, apoio, incentivos e pelo excelente ambiente que me rodeou no desenvolvimento do trabalho.

Aos meus pais e avós pela formação que deram, e à minha irmã pela paciência, apoio e boa disposição.

À Andreia pelo apoio, incentivo e compreensão ao longo do desenvolvimento de todo este trabalho, e por tudo o que representa para mim.

Referências Bibliográficas

[1] Clemm, A. (2006). Network Management Fundamentals: A guide to understand how network management technology really works. Cisco Press.

[2] Badger, M. (2008). Zenoss Core - Network and System Monitoring: A step-by-step guide to configuring, using, and adapting the free open-source network monitoring system. Packt Publishing.

[3]Portal do Netsaint. Disponível em: http://web.archive.org/web/20011210172354/www.netsaint.org/docs/0_0_7/about.html#whatis

[4] http://web.archive.org/web/20010714091800/http://www.nagios.org/

[5] Extensões para a ferramenta Nagios. Disponível em: http://exchange.nagios.org/

[6] Schubert, Max; Bennet, Derrick; Gines, Jonathan; Hay, Andrew; Strand, John (2008). Nagios 3 Enterprise Network Monitoring including Plug-Ins and Hardware Devices. Syngress.

[7] Kundi, Dinangkur; Lavlu, S.M. Ibrahim (2009). Cacti 0.8 Network Monitoring. PACKT Publishing.

[8] Boutaba, Raouf; Polyrakis, Andreas (2001). Projecting FCAPS to Active Networks.

[9]Goyal, Pankaj; Mikkilineni; Ganti,Murthy (2009). FCAPS in the Business Services Fabric Model.

[10] Modelo funcional da gestão de redes. Disponível em: http://www.networkdictionary.com/networking/FCAPS.php

[11]Burgess, Chris (2005). The Nagios Book. Chris Burgess.

[12]Turnbull, James(2006). Pro Nagios 2.0. Apress.

[13]Galstad, Ethan(2007). NRPE Documentation.

[14]S. Berner, Eta (2007). Clinical Decision Support Systems – Theory and Pratice. Springer.

[15] Druzdzel, Mark J.;Flynn, Roger R. (2002). Decision Support Systems.

[16]Formoso, Vreixo; Cacheda, Fidel; Carneiro, Víctor; Valiño, Juan. Open Source Tool for Management Network Information.

[17]Allen, Hervey; Regnauld, Phil; Smith, Dale (2008). Campus Network Best Practices: Network Management & Monitoring Overview.

[18]Davis, Thomas; Skinner, David. System Monitoring Using Nagios, Cacti, and Prism.

[19]Stelte, Bjorn; Hochstatter, Iris. iNagMon – Network Monitoring on the iPhone.

[20]Silver, T.Michael (2009). Monitoring Network and Service Availability with Open-Source Software

[21]Seglie, Scott V. (2001). Network Monitoring with Nagios.

[22]Meier, Adriano M.; de Macedo, Douglas D. J.; Righi, Rafael R.; Kreutz, Diego L.; Dantas, M. A.R.. Um Estudo Comparativo de Ferramentas Baseadas em Código Livre para o Controle e Monitoramento de Redes.